	P192 K163 B163	P224 K233 B233	P256 K283 B283	P384 K409 B409	P521 K571 B571
Hash algorithm	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Hash length	160	224	256	384	512
KDF	Concatenation KDF				
Derived Key Material length	320	448	512	768	1024
MacKey length	80	112	128	192	256
MacTag length	160	224	256	384	512
ID_U	"ALICE"				
ID_V	"BOBBY"				
Message Strings (Unilateral)	KC_1_U KC_1_V				
Message Strings (Bilateral)	KC_2_U KC_2_V				

OtherInfo for KDF

AlgorithmID	123456789ABCDEF0
PartyUInfo	414C494345313233
PartyVInfo	424F424259343536
SupPubInfo	not used

OtherInfo for KDF (StaticUnifiedModel) requires the PartyUInfo to contain a nonce therefore the value is:

PartyUInfo = 414C494345313233 || nonceU_byte_len || nonceU

FullUnifiedCDH(P-192)
---
dsU is
        20F234D3 2CD7EDD8 BFC5BD96 DAE60859 3E38E894 2324FDE8

QsU_x is
        896C0B5E E70F55B3 B463101C 1BFB86D3 A7C6C5DA 354F6214

QsU_y is
        40B85F14 4536C6F5 4BC85BED 3820A74A BF58BC78 2D1DB241

dsV is
        0F9E539A E24C3A90 5B4ED7CE 4E2EBAD4 E4B77491 2623284B

QsV_x is
        09F9D21C 7FD98D09 7B4C3AE7 64300040 3DB445B7 49C4B441

QsV_y is
        43CB6933 62FD117C 79F255D9 DD6BBE75 F43BE57D 14E28685

deU is
        323FA316 9D8E9C65 93F59476 BC142000 AB5BE0E2 49C43426

QeU_x is
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612

QeU_y is
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A

deV is
        631F95BB 4A67632C 9C476EEE 9AB695AB 240A0499 307FCF62

QeV_x is
        519A1216 80E00454 66BA21DF 2EEE47F5 973B5005 77EF13D5

QeV_y is
        FF613AB4 D64CEE3A 20875BDB 10F953F6 B30CA072 C60AA57F

---

no Key Confirmation
Zs is
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D

Ze is
        AD420182 633F8526 BFE954AC DA376F05 E5FF4F83 7F54FEBE

Z is
        AD420182 633F8526 BFE954AC DA376F05 E5FF4F83 7F54FEBE
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                         6FEF442F C17A7E2B 0C9DECE0 E47A5748
        ACB46AF1 98D76747 0F28A104 B56130AE B01009A4 5682A5E1

KeyData is
                         6FEF442F C17A7E2B 0C9DECE0 E47A5748
        ACB46AF1 98D76747 0F28A104 B56130AE B01009A4 5682A5E1

Scheme Initiator, Key Confirmation Provider: U to V
Zs is
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D

Ze is

```
        AD420182 633F8526 BFE954AC DA376F05 E5FF4F83 7F54FEBE


Z is
        AD420182 633F8526 BFE954AC DA376F05 E5FF4F83 7F54FEBE
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            6FEF
        442FC17A 7E2B0C9D ECE0E47A 5748ACB4 6AF198D7 67470F28
        A104B561 30AEB010 09A45682 A5E17D62 1894ADB8 ADDCFE57


MacData is
                         4B435F31 5F55414C 49434542 4F424259
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A
        519A1216 80E00454 66BA21DF 2EEE47F5 973B5005 77EF13D5
        FF613AB4 D64CEE3A 20875BDB 10F953F6 B30CA072 C60AA57F


MacKey is
                                       6FEF 442FC17A 7E2B0C9D


Mtag is
                 9FC2821F 2F0314E6 7D4ED678 F9F53409 E50F0B6C


KeyData is
                         ECE0E47A 5748ACB4 6AF198D7 67470F28
        A104B561 30AEB010 09A45682 A5E17D62 1894ADB8 ADDCFE57




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Zs is
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D
```

```
Ze is
        AD420182 633F8526 BFE954AC DA376F05 E5FF4F83 7F54FEBE


Z is
        AD420182 633F8526 BFE954AC DA376F05 E5FF4F83 7F54FEBE
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            6FEF
        442FC17A 7E2B0C9D ECE0E47A 5748ACB4 6AF198D7 67470F28
        A104B561 30AEB010 09A45682 A5E17D62 1894ADB8 ADDCFE57


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        519A1216 80E00454 66BA21DF 2EEE47F5 973B5005 77EF13D5
        FF613AB4 D64CEE3A 20875BDB 10F953F6 B30CA072 C60AA57F
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A


MacKey is
                                       6FEF 442FC17A 7E2B0C9D


Mtag is
                 8CFF7B69 2AD54B6E 72310512 31EC449D 177B75B5


KeyData is
                         ECE0E47A 5748ACB4 6AF198D7 67470F28
        A104B561 30AEB010 09A45682 A5E17D62 1894ADB8 ADDCFE57




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
Zs is
```

```
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


Ze is
        AD420182 633F8526 BFE954AC DA376F05 E5FF4F83 7F54FEBE


Z is
        AD420182 633F8526 BFE954AC DA376F05 E5FF4F83 7F54FEBE
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            6FEF
        442FC17A 7E2B0C9D ECE0E47A 5748ACB4 6AF198D7 67470F28
        A104B561 30AEB010 09A45682 A5E17D62 1894ADB8 ADDCFE57


U2V
----------------
MacData is
                          4B435F32 5F55414C 49434542 4F424259
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A
        519A1216 80E00454 66BA21DF 2EEE47F5 973B5005 77EF13D5
        FF613AB4 D64CEE3A 20875BDB 10F953F6 B30CA072 C60AA57F


MacKey is
                                       6FEF 442FC17A 7E2B0C9D


Mtag is
                0C095ACF 86073288 9A1AE24E E016A615 0DEEC052


V2U
----------------
MacData is
                          4B435F32 5F56424F 42425941 4C494345
        519A1216 80E00454 66BA21DF 2EEE47F5 973B5005 77EF13D5
        FF613AB4 D64CEE3A 20875BDB 10F953F6 B30CA072 C60AA57F
```

CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A

MacKey is
6FEF 442FC17A 7E2B0C9D

Mtag is
5A0177D4 BF7EA587 E1A463BC 8A621FE8 F1DAAF5E

KeyData is
ECE0E47A 5748ACB4 6AF198D7 67470F28
A104B561 30AEB010 09A45682 A5E17D62 1894ADB8 ADDCFE57

FullMQV(P-192)
---
dsU is
20F234D3 2CD7EDD8 BFC5BD96 DAE60859 3E38E894 2324FDE8

QsU_x is
896C0B5E E70F55B3 B463101C 1BFB86D3 A7C6C5DA 354F6214

QsU_y is
40B85F14 4536C6F5 4BC85BED 3820A74A BF58BC78 2D1DB241

dsV is
0F9E539A E24C3A90 5B4ED7CE 4E2EBAD4 E4B77491 2623284B

QsV_x is
09F9D21C 7FD98D09 7B4C3AE7 64300040 3DB445B7 49C4B441

QsV_y is
43CB6933 62FD117C 79F255D9 DD6BBE75 F43BE57D 14E28685

deU is

```
        323FA316 9D8E9C65 93F59476 BC142000 AB5BE0E2 49C43426


QeU_x is
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612


QeU_y is
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A


deV is
        631F95BB 4A67632C 9C476EEE 9AB695AB 240A0499 307FCF62


QeV_x is
        519A1216 80E00454 66BA21DF 2EEE47F5 973B5005 77EF13D5


QeV_y is
        FF613AB4 D64CEE3A 20875BDB 10F953F6 B30CA072 C60AA57F




------------------------------------------------------------
no Key Confirmation
Z is
        AE64AB2B 2B75A94C F8EF24DA 2456BD3A A36DB614 29EA5521


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         CC965A52 D05C949E 52C035FD 03530DB7
        EAA40870 2C9D3521 1E672154 12459151 BA2262BD 1E28E56B


KeyData is
                         CC965A52 D05C949E 52C035FD 03530DB7
        EAA40870 2C9D3521 1E672154 12459151 BA2262BD 1E28E56B
```

```
-----------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Z is
        AE64AB2B 2B75A94C F8EF24DA 2456BD3A A36DB614 29EA5521


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                          CC96
        5A52D05C 949E52C0 35FD0353 0DB7EAA4 08702C9D 35211E67
        21541245 9151BA22 62BD1E28 E56BC8BB 2271AEE7 295E6A21


MacData is
                         4B435F31 5F55414C 49434542 4F424259
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A
        519A1216 80E00454 66BA21DF 2EEE47F5 973B5005 77EF13D5
        FF613AB4 D64CEE3A 20875BDB 10F953F6 B30CA072 C60AA57F


MacKey is
                                      CC96 5A52D05C 949E52C0


Mtag is
                 BE70E818 DBCCECBD A421D5B7 DA5F0EE9 CDD62A9A


KeyData is
                         35FD0353 0DB7EAA4 08702C9D 35211E67
        21541245 9151BA22 62BD1E28 E56BC8BB 2271AEE7 295E6A21




-----------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
        AE64AB2B 2B75A94C F8EF24DA 2456BD3A A36DB614 29EA5521
```

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            CC96
        5A52D05C 949E52C0 35FD0353 0DB7EAA4 08702C9D 35211E67
        21541245 9151BA22 62BD1E28 E56BC8BB 2271AEE7 295E6A21


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        519A1216 80E00454 66BA21DF 2EEE47F5 973B5005 77EF13D5
        FF613AB4 D64CEE3A 20875BDB 10F953F6 B30CA072 C60AA57F
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A


MacKey is
                                      CC96 5A52D05C 949E52C0


Mtag is
                 9A20EA41 CE077751 1D774AC0 C3FC896E 9A5FA16E


KeyData is
                         35FD0353 0DB7EAA4 08702C9D 35211E67
        21541245 9151BA22 62BD1E28 E56BC8BB 2271AEE7 295E6A21




------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
Z is
        AE64AB2B 2B75A94C F8EF24DA 2456BD3A A36DB614 29EA5521


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            CC96
```

```
        5A52D05C 949E52C0 35FD0353 0DB7EAA4 08702C9D 35211E67
        21541245 9151BA22 62BD1E28 E56BC8BB 2271AEE7 295E6A21


U2V
----------------
MacData is
                         4B435F32 5F55414C 49434542 4F424259
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A
        519A1216 80E00454 66BA21DF 2EEE47F5 973B5005 77EF13D5
        FF613AB4 D64CEE3A 20875BDB 10F953F6 B30CA072 C60AA57F


MacKey is
                                       CC96 5A52D05C 949E52C0


Mtag is
                6C5F6913 A3BF1F7F 16386259 5C50B64B A3DE1A72


V2U
----------------
MacData is
                         4B435F32 5F56424F 42425941 4C494345
        519A1216 80E00454 66BA21DF 2EEE47F5 973B5005 77EF13D5
        FF613AB4 D64CEE3A 20875BDB 10F953F6 B30CA072 C60AA57F
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A


MacKey is
                                       CC96 5A52D05C 949E52C0


Mtag is
                B79F0184 B82652A0 E7AB0B68 2956AB3B 2330F57B


KeyData is
                         35FD0353 0DB7EAA4 08702C9D 35211E67
        21541245 9151BA22 62BD1E28 E56BC8BB 2271AEE7 295E6A21
```

EphemeralUnifiedCDH(P-192)
---
deU is
        323FA316 9D8E9C65 93F59476 BC142000 AB5BE0E2 49C43426

QeU_x is
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612

QeU_y is
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A

deV is
        631F95BB 4A67632C 9C476EEE 9AB695AB 240A0499 307FCF62

QeV_x is
        519A1216 80E00454 66BA21DF 2EEE47F5 973B5005 77EF13D5

QeV_y is
        FF613AB4 D64CEE3A 20875BDB 10F953F6 B30CA072 C60AA57F

---
no Key Confirmation
Z is
        AD420182 633F8526 BFE954AC DA376F05 E5FF4F83 7F54FEBE

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                          5F17B665 72C57B03 34BB241C E6CB3A9D
        585E5C36 257DC087 5DEE4843 56E92FAB CCE2D388 ABF7EAF0

KeyData is
                          5F17B665 72C57B03 34BB241C E6CB3A9D

585E5C36 257DC087 5DEE4843 56E92FAB CCE2D388 ABF7EAF0

OnePassUnifiedCDH(P-192)
---
dsU is
20F234D3 2CD7EDD8 BFC5BD96 DAE60859 3E38E894 2324FDE8

QsU_x is
896C0B5E E70F55B3 B463101C 1BFB86D3 A7C6C5DA 354F6214

QsU_y is
40B85F14 4536C6F5 4BC85BED 3820A74A BF58BC78 2D1DB241

dsV is
0F9E539A E24C3A90 5B4ED7CE 4E2EBAD4 E4B77491 2623284B

QsV_x is
09F9D21C 7FD98D09 7B4C3AE7 64300040 3DB445B7 49C4B441

QsV_y is
43CB6933 62FD117C 79F255D9 DD6BBE75 F43BE57D 14E28685

deU is
323FA316 9D8E9C65 93F59476 BC142000 AB5BE0E2 49C43426

QeU_x is
CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612

QeU_y is
68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A

```
no Key Confirmation
Zs is
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


Ze is
        78B3A426 67DFF154 E395367B 744CBB50 67C03D08 A96D9086


Z is
        78B3A426 67DFF154 E395367B 744CBB50 67C03D08 A96D9086
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         73D683F6 751BC092 B68F8DB2 45FBBCF8
        74A1EF99 B15E85C1 5097D9EC 246869A2 DDC8083B 52BA25FC


KeyData is
                         73D683F6 751BC092 B68F8DB2 45FBBCF8
        74A1EF99 B15E85C1 5097D9EC 246869A2 DDC8083B 52BA25FC




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309


Zs is
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


Ze is
        78B3A426 67DFF154 E395367B 744CBB50 67C03D08 A96D9086


Z is
        78B3A426 67DFF154 E395367B 744CBB50 67C03D08 A96D9086
```

```
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            73D6
        83F6751B C092B68F 8DB245FB BCF874A1 EF99B15E 85C15097
        D9EC2468 69A2DDC8 083B52BA 25FC5032 25D8C464 84EA6B82


MacData is
                          4B435F31 5F55414C 49434542 4F424259
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309


MacKey is
                                       73D6 83F6751B C092B68F


Mtag is
                 78C36193 A4ED0347 F8791C75 0DBB3360 E3691BBD


KeyData is
                          8DB245FB BCF874A1 EF99B15E 85C15097
        D9EC2468 69A2DDC8 083B52BA 25FC5032 25D8C464 84EA6B82




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309


Zs is
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


Ze is
```

```
        78B3A426 67DFF154 E395367B 744CBB50 67C03D08 A96D9086


Z is
        78B3A426 67DFF154 E395367B 744CBB50 67C03D08 A96D9086
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            73D6
        83F6751B C092B68F 8DB245FB BCF874A1 EF99B15E 85C15097
        D9EC2468 69A2DDC8 083B52BA 25FC5032 25D8C464 84EA6B82


MacData is
                          4B435F31 5F56424F 42425941 4C494345
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A


MacKey is
                                       73D6 83F6751B C092B68F


Mtag is
                 93439CD1 94CAEB81 3ECEEFFF D8FC8A5F 9D8BD4E5


KeyData is
                          8DB245FB BCF874A1 EF99B15E 85C15097
        D9EC2468 69A2DDC8 083B52BA 25FC5032 25D8C464 84EA6B82




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309


Zs is
```

```
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


Ze is
        78B3A426 67DFF154 E395367B 744CBB50 67C03D08 A96D9086


Z is
        78B3A426 67DFF154 E395367B 744CBB50 67C03D08 A96D9086
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            73D6
        83F6751B C092B68F 8DB245FB BCF874A1 EF99B15E 85C15097
        D9EC2468 69A2DDC8 083B52BA 25FC5032 25D8C464 84EA6B82


U2V
----------------
MacData is
                         4B435F32 5F55414C 49434542 4F424259
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309


MacKey is
                                       73D6 83F6751B C092B68F


Mtag is
                C12D5D7E 9318520B 9143CEF0 600D1E2E 1BD2C06D


V2U
----------------
MacData is
                         4B435F32 5F56424F 42425941 4C494345
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A
```

MacKey is
                                        73D6 83F6751B C092B68F

Mtag is
                33550A01 43DA603D E0843426 378CEDD0 E6D49C69

KeyData is
                          8DB245FB BCF874A1 EF99B15E 85C15097
        D9EC2468 69A2DDC8 083B52BA 25FC5032 25D8C464 84EA6B82

OnePassMQV(P-192)
----
dsU is
        20F234D3 2CD7EDD8 BFC5BD96 DAE60859 3E38E894 2324FDE8

QsU_x is
        896C0B5E E70F55B3 B463101C 1BFB86D3 A7C6C5DA 354F6214

QsU_y is
        40B85F14 4536C6F5 4BC85BED 3820A74A BF58BC78 2D1DB241

dsV is
        0F9E539A E24C3A90 5B4ED7CE 4E2EBAD4 E4B77491 2623284B

QsV_x is
        09F9D21C 7FD98D09 7B4C3AE7 64300040 3DB445B7 49C4B441

QsV_y is
        43CB6933 62FD117C 79F255D9 DD6BBE75 F43BE57D 14E28685

deU is
        323FA316 9D8E9C65 93F59476 BC142000 AB5BE0E2 49C43426

QeU_x is
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612

QeU_y is
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A

---
no Key Confirmation
Z is
        28D8AB53 9969B2C3 5979A92F D6462417 7A7191FF E70DE82D

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                         B291C225 89BF6962 261ECD0A 37E0AA82
        BABD90BC 9EBDFEB2 479A6859 59EB317F FCB74243 8F0FE879

KeyData is
                         B291C225 89BF6962 261ECD0A 37E0AA82
        BABD90BC 9EBDFEB2 479A6859 59EB317F FCB74243 8F0FE879

Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309

Z is
        28D8AB53 9969B2C3 5979A92F D6462417 7A7191FF E70DE82D

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

```
DerivedKeyMaterial is
                                                              B291
        C22589BF 6962261E CD0A37E0 AA82BABD 90BC9EBD FEB2479A
        685959EB 317FFCB7 42438F0F E879844C AD2594C3 15CAF548


MacData is
                         4B435F31 5F55414C 49434542 4F424259
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309


MacKey is
                                      B291 C22589BF 6962261E


Mtag is
                 B77CCEB3 AB54B2EA CD2DC61C 06A31CC1 6392D3CB


KeyData is
                         CD0A37E0 AA82BABD 90BC9EBD FEB2479A
        685959EB 317FFCB7 42438F0F E879844C AD2594C3 15CAF548




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309


Z is
        28D8AB53 9969B2C3 5979A92F D6462417 7A7191FF E70DE82D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                              B291
        C22589BF 6962261E CD0A37E0 AA82BABD 90BC9EBD FEB2479A
```

```
        685959EB 317FFCB7 42438F0F E879844C AD2594C3 15CAF548


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A


MacKey is
                                      B291 C22589BF 6962261E


Mtag is
                 07EBCB09 B4850F10 E3ABCFE4 D9825913 DBC65BA5


KeyData is
                         CD0A37E0 AA82BABD 90BC9EBD FEB2479A
        685959EB 317FFCB7 42438F0F E879844C AD2594C3 15CAF548




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309


Z is
        28D8AB53 9969B2C3 5979A92F D6462417 7A7191FF E70DE82D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                          B291
        C22589BF 6962261E CD0A37E0 AA82BABD 90BC9EBD FEB2479A
        685959EB 317FFCB7 42438F0F E879844C AD2594C3 15CAF548


U2V
----------------
```

```
MacData is
                        4B435F32 5F55414C 49434542 4F424259
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309


MacKey is
                                     B291 C22589BF 6962261E


Mtag is
                CD5B865D 6B5C4ED0 6F50D438 5EDDA5EB 87BE7907


V2U
----------------
MacData is
                        4B435F32 5F56424F 42425941 4C494345
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A


MacKey is
                                     B291 C22589BF 6962261E


Mtag is
                D5B5AA11 A2679DA4 6556463E 4F4B4390 D3EA7337


KeyData is
                        CD0A37E0 AA82BABD 90BC9EBD FEB2479A
        685959EB 317FFCB7 42438F0F E879844C AD2594C3 15CAF548




OnePassDiffieHellmanCDH(P-192)
------------------------------------------------------------
dsV is
        0F9E539A E24C3A90 5B4ED7CE 4E2EBAD4 E4B77491 2623284B


QsV_x is
```

```
        09F9D21C 7FD98D09 7B4C3AE7 64300040 3DB445B7 49C4B441


QsV_y is
        43CB6933 62FD117C 79F255D9 DD6BBE75 F43BE57D 14E28685


deU is
        323FA316 9D8E9C65 93F59476 BC142000 AB5BE0E2 49C43426


QeU_x is
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612


QeU_y is
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A




------------------------------------------------------------
no Key Confirmation
Z is
        78B3A426 67DFF154 E395367B 744CBB50 67C03D08 A96D9086


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         1811595A AE8280AE 98CAC5D7 D8ABCFB8
        12EF12BA F7241C8C DAC23476 F82967A9 B0A87754 98F39B63


KeyData is
                         1811595A AE8280AE 98CAC5D7 D8ABCFB8
        12EF12BA F7241C8C DAC23476 F82967A9 B0A87754 98F39B63




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
```

```
        78B3A426 67DFF154 E395367B 744CBB50 67C03D08 A96D9086


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            1811
        595AAE82 80AE98CA C5D7D8AB CFB812EF 12BAF724 1C8CDAC2
        3476F829 67A9B0A8 775498F3 9B633200 E1C0DF52 C65BC142


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A


MacKey is
                                      1811 595AAE82 80AE98CA


Mtag is
                650B63C0 625A62AF FC741CAF 57F945EE F1F7B36C


KeyData is
                         C5D7D8AB CFB812EF 12BAF724 1C8CDAC2
        3476F829 67A9B0A8 775498F3 9B633200 E1C0DF52 C65BC142




StaticUnifiedCDH(P-192)
------------------------------------------------------------
dsU is
        20F234D3 2CD7EDD8 BFC5BD96 DAE60859 3E38E894 2324FDE8


QsU_x is
        896C0B5E E70F55B3 B463101C 1BFB86D3 A7C6C5DA 354F6214


QsU_y is
        40B85F14 4536C6F5 4BC85BED 3820A74A BF58BC78 2D1DB241
```

```
dsV is
        0F9E539A E24C3A90 5B4ED7CE 4E2EBAD4 E4B77491 2623284B


QsV_x is
        09F9D21C 7FD98D09 7B4C3AE7 64300040 3DB445B7 49C4B441


QsV_y is
        43CB6933 62FD117C 79F255D9 DD6BBE75 F43BE57D 14E28685




------------------------------------------------------------
no Key Confirmation
NonceU is
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309


Z is
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


OtherInfo is
                                                          1234
        56789ABC DEF0414C 49434531 3233C000 F8C1FC06 6B3EABFE
        0048466C A80DFDFB A3B9F7C3 73173309 424F4242 59343536


DerivedKeyMaterial is
                          97D227DD 8E001BFC 58AC4933 1C2233D8
        8128422F 35D247F1 68A2813B AAECB3AA E0F84155 7885E446


KeyData is
                          97D227DD 8E001BFC 58AC4933 1C2233D8
        8128422F 35D247F1 68A2813B AAECB3AA E0F84155 7885E446




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
```

```
NonceU is
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309


NonceV is
        81DB7325 97393873 89E51893 EFAD98A0 F0442D34 A531DC53


Z is
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


OtherInfo is
                                                            1234
        56789ABC DEF0414C 49434531 3233C000 F8C1FC06 6B3EABFE
        0048466C A80DFDFB A3B9F7C3 73173309 424F4242 59343536


DerivedKeyMaterial is
                                                          97D2
        27DD8E00 1BFC58AC 49331C22 33D88128 422F35D2 47F168A2
        813BAAEC B3AAE0F8 41557885 E446E549 0A21E789 7277A6D7


MacData is
                         4B435F31 5F55414C 49434542 4F424259
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309
        81DB7325 97393873 89E51893 EFAD98A0 F0442D34 A531DC53


MacKey is
                                       97D2 27DD8E00 1BFC58AC


Mtag is
                525878C5 3D2851E1 1355A221 DBA01855 99B13388


KeyData is
                         49331C22 33D88128 422F35D2 47F168A2
        813BAAEC B3AAE0F8 41557885 E446E549 0A21E789 7277A6D7
```

Scheme Responder, Key Confirmation Provider: V to U
NonceV is
        81DB7325 97393873 89E51893 EFAD98A0 F0442D34 A531DC53

NonceU is
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309

Z is
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D

OtherInfo is
                                                            1234
        56789ABC DEF0414C 49434531 3233C000 F8C1FC06 6B3EABFE
        0048466C A80DFDFB A3B9F7C3 73173309 424F4242 59343536

DerivedKeyMaterial is
                                                          97D2
        27DD8E00 1BFC58AC 49331C22 33D88128 422F35D2 47F168A2
        813BAAEC B3AAE0F8 41557885 E446E549 0A21E789 7277A6D7

MacData is
                          4B435F31 5F56424F 42425941 4C494345
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309

MacKey is
                                      97D2 27DD8E00 1BFC58AC

Mtag is
                 9EBA877C 4B6D62AE 22A9ED34 5280F5B1 A28421FF

KeyData is
                          49331C22 33D88128 422F35D2 47F168A2
        813BAAEC B3AAE0F8 41557885 E446E549 0A21E789 7277A6D7

```
Scheme Initiator, Key Confirmation Bilateral
NonceU is
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309


NonceV is
        81DB7325 97393873 89E51893 EFAD98A0 F0442D34 A531DC53


Z is
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


OtherInfo is
                                                            1234
        56789ABC DEF0414C 49434531 3233C000 F8C1FC06 6B3EABFE
        0048466C A80DFDFB A3B9F7C3 73173309 424F4242 59343536


DerivedKeyMaterial is
                                                          97D2
        27DD8E00 1BFC58AC 49331C22 33D88128 422F35D2 47F168A2
        813BAAEC B3AAE0F8 41557885 E446E549 0A21E789 7277A6D7


U2V
----------------
MacData is
                          4B435F32 5F55414C 49434542 4F424259
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309
        81DB7325 97393873 89E51893 EFAD98A0 F0442D34 A531DC53


MacKey is
                                       97D2 27DD8E00 1BFC58AC


Mtag is
                F563A1FF F1D386F2 AD2A5FAE 42D60BE7 5858ABD0


V2U
----------------
MacData is
                          4B435F32 5F56424F 42425941 4C494345
```

81DB7325 97393873 89E51893 EFAD98A0 F0442D34 A531DC53
F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309

MacKey is

97D2 27DD8E00 1BFC58AC

Mtag is

C64C12EF 4D9FDB90 0B24EA6C 92E7E4B4 CB07E81E

KeyData is

49331C22 33D88128 422F35D2 47F168A2
813BAAEC B3AAE0F8 41557885 E446E549 0A21E789 7277A6D7

FullUnifiedCDH(P-224)
----
dsU is
                                                        A273DD64
        3AB8A64B 4B6E1FF9 C7ECF18E BC1F62DE 33450A9E 32E8A504

QsU_x is
                                                        FAD43A96
        46721C46 52F13752 345FC2D5 25515A55 A170E685 314810E1

QsU_y is
                                                        E05BE902
        7238C138 7F7C5575 ED425324 32929EFB C2C37293 1253F3D2

dsV is
                                                        723A6551
        09089ED0 EDB4E630 72A82640 9F9C6204 635169F0 681F7514

QsV_x is
                                                        0898B1C4
        B9308496 45F2E605 00DA0492 0CB70272 3E4E13F6 64C99B0B

QsV_y is
                                                        0D91CF88
        A13435E4 D126DA64 352C75F2 B80C65F9 43D6F65A 6AC20F0B

deU is
                                                        B558EB6C
        288DA707 BBB4F8FB AE2AB9E9 CB62E3BC 5C7573E2 2E26D37F

QeU_x is
                                                        49DFEF30
        9F81488C 304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB

QeU_y is
                                                        4F2B5EE4

5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4

deV is
AC3B1ADD
3D9770E6 F6A708EE 9F3B8E0A B3B480E9 F27F85C8 8B5E6D18

QeV_x is
6B3AC96A
8D0CDE6A 5599BE80 32EDF10C 162D0A8A D219506D CD42A207

QeV_y is
D491BE99
C213A7D1 CA3706DE BFE305F3 61AFCBB3 3E2609C8 B1618AD5

---

no Key Confirmation
Zs is
9F18FF54
F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9

Ze is
52272F50
F46F4EDC 91515690 92F46DF2 D96ECC3B 6DC1714A 4EA949FA

Z is
52272F50 F46F4EDC
91515690 92F46DF2 D96ECC3B 6DC1714A 4EA949FA 9F18FF54
F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
7756BCFD EF3EE69F
6AC23CD2 DC607D01 FA8CE1B2 4F5CAAAA 48E04B81 63E1733A
ED7A040E 73F2B542 368F0054 8B163C3D C96D7009 9916F16B

KeyData is
                                                7756BCFD EF3EE69F
        6AC23CD2 DC607D01 FA8CE1B2 4F5CAAAA 48E04B81 63E1733A
        ED7A040E 73F2B542 368F0054 8B163C3D C96D7009 9916F16B

Scheme Initiator, Key Confirmation Provider: U to V
Zs is
                                                        9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9

Ze is
                                                        52272F50
        F46F4EDC 91515690 92F46DF2 D96ECC3B 6DC1714A 4EA949FA

Z is
                                                52272F50 F46F4EDC
        91515690 92F46DF2 D96ECC3B 6DC1714A 4EA949FA 9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
            7756 BCFDEF3E E69F6AC2 3CD2DC60 7D01FA8C E1B24F5C
        AAAA48E0 4B8163E1 733AED7A 040E73F2 B542368F 00548B16
        3C3DC96D 70099916 F16B96DE 6EF4948D 3C2EF037 E45DCD43

MacData is
                                                4B435F31 5F55414C
        49434542 4F424259 49DFEF30 9F81488C 304CFF5A B3EE5A21
        54367DC7 833150E0 A51F3EEB 4F2B5EE4 5762C4F6 54C1A0C6
        7F54CF88 B016B51B CE3D7C22 8D57ADB4 6B3AC96A 8D0CDE6A
        5599BE80 32EDF10C 162D0A8A D219506D CD42A207 D491BE99
        C213A7D1 CA3706DE BFE305F3 61AFCBB3 3E2609C8 B1618AD5

MacKey is
                              7756 BCFDEF3E E69F6AC2 3CD2DC60

Mtag is
                                                        9EE6013E
        119F3782 BF892E92 9E04D14D D24BDD0F 28FB87FC BE37803E

KeyData is
                                               7D01FA8C E1B24F5C
        AAAA48E0 4B8163E1 733AED7A 040E73F2 B542368F 00548B16
        3C3DC96D 70099916 F16B96DE 6EF4948D 3C2EF037 E45DCD43

Scheme Responder, Key Confirmation Provider: V to U
Zs is
                                                        9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9

Ze is
                                                        52272F50
        F46F4EDC 91515690 92F46DF2 D96ECC3B 6DC1714A 4EA949FA

Z is
                                               52272F50 F46F4EDC
        91515690 92F46DF2 D96ECC3B 6DC1714A 4EA949FA 9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
            7756 BCFDEF3E E69F6AC2 3CD2DC60 7D01FA8C E1B24F5C
        AAAA48E0 4B8163E1 733AED7A 040E73F2 B542368F 00548B16
        3C3DC96D 70099916 F16B96DE 6EF4948D 3C2EF037 E45DCD43

MacData is
                                                4B435F31 5F56424F
        42425941 4C494345 6B3AC96A 8D0CDE6A 5599BE80 32EDF10C
        162D0A8A D219506D CD42A207 D491BE99 C213A7D1 CA3706DE
        BFE305F3 61AFCBB3 3E2609C8 B1618AD5 49DFEF30 9F81488C
        304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4
        5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4

MacKey is
                             7756 BCFDEF3E E69F6AC2 3CD2DC60

Mtag is
                                                        32FB2425
        20A67C16 52658556 16754B36 488841C8 B141EDB9 2F2B8400

KeyData is
                                                7D01FA8C E1B24F5C
        AAAA48E0 4B8163E1 733AED7A 040E73F2 B542368F 00548B16
        3C3DC96D 70099916 F16B96DE 6EF4948D 3C2EF037 E45DCD43

Scheme Initiator, Key Confirmation Bilateral
Zs is
                                                        9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9

Ze is
                                                        52272F50
        F46F4EDC 91515690 92F46DF2 D96ECC3B 6DC1714A 4EA949FA

Z is
                                                52272F50 F46F4EDC
        91515690 92F46DF2 D96ECC3B 6DC1714A 4EA949FA 9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

```
DerivedKeyMaterial is
            7756 BCFDEF3E E69F6AC2 3CD2DC60 7D01FA8C E1B24F5C
         AAAA48E0 4B8163E1 733AED7A 040E73F2 B542368F 00548B16
         3C3DC96D 70099916 F16B96DE 6EF4948D 3C2EF037 E45DCD43


U2V
----------------
MacData is
                                              4B435F32 5F55414C
         49434542 4F424259 49DFEF30 9F81488C 304CFF5A B3EE5A21
         54367DC7 833150E0 A51F3EEB 4F2B5EE4 5762C4F6 54C1A0C6
         7F54CF88 B016B51B CE3D7C22 8D57ADB4 6B3AC96A 8D0CDE6A
         5599BE80 32EDF10C 162D0A8A D219506D CD42A207 D491BE99
         C213A7D1 CA3706DE BFE305F3 61AFCBB3 3E2609C8 B1618AD5


MacKey is
                              7756 BCFDEF3E E69F6AC2 3CD2DC60


Mtag is
                                                      3C1B7182
         FF32DC91 BCD26B90 223CDC27 34EBF8CC 236EB944 857153B2


V2U
----------------
MacData is
                                              4B435F32 5F56424F
         42425941 4C494345 6B3AC96A 8D0CDE6A 5599BE80 32EDF10C
         162D0A8A D219506D CD42A207 D491BE99 C213A7D1 CA3706DE
         BFE305F3 61AFCBB3 3E2609C8 B1618AD5 49DFEF30 9F81488C
         304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4
         5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4


MacKey is
                              7756 BCFDEF3E E69F6AC2 3CD2DC60


Mtag is
                                                      7DFA15A7
         5550A8FD F01AF1EF 77FB9547 7E49D672 6CFD3BD1 079428CA
```

KeyData is
                                                7D01FA8C E1B24F5C
        AAAA48E0 4B8163E1 733AED7A 040E73F2 B542368F 00548B16
        3C3DC96D 70099916 F16B96DE 6EF4948D 3C2EF037 E45DCD43

FullMQV(P-224)
----
dsU is
                                                        A273DD64
        3AB8A64B 4B6E1FF9 C7ECF18E BC1F62DE 33450A9E 32E8A504

QsU_x is
                                                        FAD43A96
        46721C46 52F13752 345FC2D5 25515A55 A170E685 314810E1

QsU_y is
                                                        E05BE902
        7238C138 7F7C5575 ED425324 32929EFB C2C37293 1253F3D2

dsV is
                                                        723A6551
        09089ED0 EDB4E630 72A82640 9F9C6204 635169F0 681F7514

QsV_x is
                                                        0898B1C4
        B9308496 45F2E605 00DA0492 0CB70272 3E4E13F6 64C99B0B

QsV_y is
                                                        0D91CF88
        A13435E4 D126DA64 352C75F2 B80C65F9 43D6F65A 6AC20F0B

deU is
                                                        B558EB6C
        288DA707 BBB4F8FB AE2AB9E9 CB62E3BC 5C7573E2 2E26D37F

```
QeU_x is
                                                        49DFEF30
        9F81488C 304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB


QeU_y is
                                                        4F2B5EE4
        5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4


deV is
                                                        AC3B1ADD
        3D9770E6 F6A708EE 9F3B8E0A B3B480E9 F27F85C8 8B5E6D18


QeV_x is
                                                        6B3AC96A
        8D0CDE6A 5599BE80 32EDF10C 162D0A8A D219506D CD42A207


QeV_y is
                                                        D491BE99
        C213A7D1 CA3706DE BFE305F3 61AFCBB3 3E2609C8 B1618AD5




-------------------------------------------------------------
no Key Confirmation
Z is
                                                        DEF3B660
        18D14DCD FFF1C251 174C6825 82709092 5AA823EF A0F99812


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                5924621F C51249E4
        48BBF95B B47E6B6B 6406F8E1 A1E1C046 C6B4F49C 4DD866F3
        F76A47C4 C996BCA3 0B02789A 023DFCB4 1270EAB2 A1F10B00


KeyData is
```

```
                                                5924621F C51249E4
        48BBF95B B47E6B6B 6406F8E1 A1E1C046 C6B4F49C 4DD866F3
        F76A47C4 C996BCA3 0B02789A 023DFCB4 1270EAB2 A1F10B00



------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Z is
                                                        DEF3B660
        18D14DCD FFF1C251 174C6825 82709092 5AA823EF A0F99812


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            5924 621FC512 49E448BB F95BB47E 6B6B6406 F8E1A1E1
        C046C6B4 F49C4DD8 66F3F76A 47C4C996 BCA30B02 789A023D
        FCB41270 EAB2A1F1 0B00A4E0 3C6F0379 624382F0 3C4F340A


MacData is
                                                4B435F31 5F55414C
        49434542 4F424259 49DFEF30 9F81488C 304CFF5A B3EE5A21
        54367DC7 833150E0 A51F3EEB 4F2B5EE4 5762C4F6 54C1A0C6
        7F54CF88 B016B51B CE3D7C22 8D57ADB4 6B3AC96A 8D0CDE6A
        5599BE80 32EDF10C 162D0A8A D219506D CD42A207 D491BE99
        C213A7D1 CA3706DE BFE305F3 61AFCBB3 3E2609C8 B1618AD5


MacKey is
                              5924 621FC512 49E448BB F95BB47E


Mtag is
                                                        6FA28E3D
        AB50C637 65039C64 ED28C014 AF9AE6FB FC0E633A 4748CAE4


KeyData is
                                                6B6B6406 F8E1A1E1
        C046C6B4 F49C4DD8 66F3F76A 47C4C996 BCA30B02 789A023D
        FCB41270 EAB2A1F1 0B00A4E0 3C6F0379 624382F0 3C4F340A
```

```
-------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
                                                        DEF3B660
        18D14DCD FFF1C251 174C6825 82709092 5AA823EF A0F99812


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            5924 621FC512 49E448BB F95BB47E 6B6B6406 F8E1A1E1
        C046C6B4 F49C4DD8 66F3F76A 47C4C996 BCA30B02 789A023D
        FCB41270 EAB2A1F1 0B00A4E0 3C6F0379 624382F0 3C4F340A


MacData is
                                               4B435F31 5F56424F
        42425941 4C494345 6B3AC96A 8D0CDE6A 5599BE80 32EDF10C
        162D0A8A D219506D CD42A207 D491BE99 C213A7D1 CA3706DE
        BFE305F3 61AFCBB3 3E2609C8 B1618AD5 49DFEF30 9F81488C
        304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4
        5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4


MacKey is
                              5924 621FC512 49E448BB F95BB47E


Mtag is
                                                        A22C1AC7
        613C91C9 E3F85F55 7DA051FC 59C42F35 53132A10 DB641373


KeyData is
                                               6B6B6406 F8E1A1E1
        C046C6B4 F49C4DD8 66F3F76A 47C4C996 BCA30B02 789A023D
        FCB41270 EAB2A1F1 0B00A4E0 3C6F0379 624382F0 3C4F340A
```

```
-----------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
Z is
                                                        DEF3B660
        18D14DCD FFF1C251 174C6825 82709092 5AA823EF A0F99812


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            5924 621FC512 49E448BB F95BB47E 6B6B6406 F8E1A1E1
        C046C6B4 F49C4DD8 66F3F76A 47C4C996 BCA30B02 789A023D
        FCB41270 EAB2A1F1 0B00A4E0 3C6F0379 624382F0 3C4F340A


U2V
----------------
MacData is
                                            4B435F32 5F55414C
        49434542 4F424259 49DFEF30 9F81488C 304CFF5A B3EE5A21
        54367DC7 833150E0 A51F3EEB 4F2B5EE4 5762C4F6 54C1A0C6
        7F54CF88 B016B51B CE3D7C22 8D57ADB4 6B3AC96A 8D0CDE6A
        5599BE80 32EDF10C 162D0A8A D219506D CD42A207 D491BE99
        C213A7D1 CA3706DE BFE305F3 61AFCBB3 3E2609C8 B1618AD5


MacKey is
                              5924 621FC512 49E448BB F95BB47E


Mtag is
                                                        A18A79FC
        B60D7368 ABA1D3FC 80D3D745 2678EA16 0734453A 208FAF61


V2U
----------------
MacData is
                                            4B435F32 5F56424F
        42425941 4C494345 6B3AC96A 8D0CDE6A 5599BE80 32EDF10C
        162D0A8A D219506D CD42A207 D491BE99 C213A7D1 CA3706DE
        BFE305F3 61AFCBB3 3E2609C8 B1618AD5 49DFEF30 9F81488C
```

```
        304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4
        5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4


MacKey is
                             5924 621FC512 49E448BB F95BB47E


Mtag is
                                                    DB375DC5
        2BA00B86 1B5F365D 41CDED7D 3AAFCE42 576F1301 1183AC41


KeyData is
                                                6B6B6406 F8E1A1E1
        C046C6B4 F49C4DD8 66F3F76A 47C4C996 BCA30B02 789A023D
        FCB41270 EAB2A1F1 0B00A4E0 3C6F0379 624382F0 3C4F340A




EphemeralUnifiedCDH(P-224)
----------------------------------------------------------
deU is
                                                    B558EB6C
        288DA707 BBB4F8FB AE2AB9E9 CB62E3BC 5C7573E2 2E26D37F


QeU_x is
                                                    49DFEF30
        9F81488C 304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB


QeU_y is
                                                    4F2B5EE4
        5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4


deV is
                                                    AC3B1ADD
        3D9770E6 F6A708EE 9F3B8E0A B3B480E9 F27F85C8 8B5E6D18


QeV_x is
                                                    6B3AC96A
        8D0CDE6A 5599BE80 32EDF10C 162D0A8A D219506D CD42A207
```

```
QeV_y is
                                                        D491BE99
        C213A7D1 CA3706DE BFE305F3 61AFCBB3 3E2609C8 B1618AD5




------------------------------------------------------------
no Key Confirmation
Z is
                                                        52272F50
        F46F4EDC 91515690 92F46DF2 D96ECC3B 6DC1714A 4EA949FA


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                8F61E07C 6B90ECD0
        15E5DED9 ED3B82B8 229786BD FB039289 CC666FAD 99E0D042
        A3F19045 8335A703 26486A23 43DBB074 0984604F 1E715BEE


KeyData is
                                                8F61E07C 6B90ECD0
        15E5DED9 ED3B82B8 229786BD FB039289 CC666FAD 99E0D042
        A3F19045 8335A703 26486A23 43DBB074 0984604F 1E715BEE




OnePassUnifiedCDH(P-224)
------------------------------------------------------------
dsU is
                                                        A273DD64
        3AB8A64B 4B6E1FF9 C7ECF18E BC1F62DE 33450A9E 32E8A504


QsU_x is
                                                        FAD43A96
        46721C46 52F13752 345FC2D5 25515A55 A170E685 314810E1
```

```
QsU_y is
                                                        E05BE902
        7238C138 7F7C5575 ED425324 32929EFB C2C37293 1253F3D2


dsV is
                                                        723A6551
        09089ED0 EDB4E630 72A82640 9F9C6204 635169F0 681F7514


QsV_x is
                                                        0898B1C4
        B9308496 45F2E605 00DA0492 0CB70272 3E4E13F6 64C99B0B


QsV_y is
                                                        0D91CF88
        A13435E4 D126DA64 352C75F2 B80C65F9 43D6F65A 6AC20F0B


deU is
                                                        B558EB6C
        288DA707 BBB4F8FB AE2AB9E9 CB62E3BC 5C7573E2 2E26D37F


QeU_x is
                                                        49DFEF30
        9F81488C 304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB


QeU_y is
                                                        4F2B5EE4
        5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4




------------------------------------------------------------
no Key Confirmation
Zs is
                                                        9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9


Ze is
                                                        59141E22
```

```
        76D41EDA D4E6D088 5C363DCF E91FCC0C 1726D11C FB3AA35B


Z is
                                                59141E22 76D41EDA
        D4E6D088 5C363DCF E91FCC0C 1726D11C FB3AA35B 9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                92EA706A 6FCE4DD2
        0D0B918B C1076EEE 1FBCD591 37429C8B 56B201D3 D7255180
        E8F11FF1 DBB34C10 310028E0 29708B05 0A834422 934109BD


KeyData is
                                                92EA706A 6FCE4DD2
        0D0B918B C1076EEE 1FBCD591 37429C8B 56B201D3 D7255180
        E8F11FF1 DBB34C10 310028E0 29708B05 0A834422 934109BD




-------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                                                        4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9


Zs is
                                                        9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9


Ze is
                                                        59141E22
        76D41EDA D4E6D088 5C363DCF E91FCC0C 1726D11C FB3AA35B


Z is
                                                59141E22 76D41EDA
```

```
        D4E6D088 5C363DCF E91FCC0C 1726D11C FB3AA35B 9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            92EA 706A6FCE 4DD20D0B 918BC107 6EEE1FBC D5913742
        9C8B56B2 01D3D725 5180E8F1 1FF1DBB3 4C103100 28E02970
        8B050A83 44229341 09BD0362 8FC0BA70 8AA035DB B2D8C4F0


MacData is
                                                        4B435F31
        5F55414C 49434542 4F424259 49DFEF30 9F81488C 304CFF5A
        B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4 5762C4F6
        54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4 4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9


MacKey is
                               92EA 706A6FCE 4DD20D0B 918BC107


Mtag is
                                                        083B64E0
        F6BAAA1D D69B4545 E42CEF3F 9C292D80 0DCA76D1 7E71E687


KeyData is
                                                6EEE1FBC D5913742
        9C8B56B2 01D3D725 5180E8F1 1FF1DBB3 4C103100 28E02970
        8B050A83 44229341 09BD0362 8FC0BA70 8AA035DB B2D8C4F0




-----------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
                                                        4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9
```

```
Zs is
                                                        9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9


Ze is
                                                        59141E22
        76D41EDA D4E6D088 5C363DCF E91FCC0C 1726D11C FB3AA35B


Z is
                                            59141E22 76D41EDA
        D4E6D088 5C363DCF E91FCC0C 1726D11C FB3AA35B 9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            92EA 706A6FCE 4DD20D0B 918BC107 6EEE1FBC D5913742
        9C8B56B2 01D3D725 5180E8F1 1FF1DBB3 4C103100 28E02970
        8B050A83 44229341 09BD0362 8FC0BA70 8AA035DB B2D8C4F0


MacData is
        4B435F31 5F56424F 42425941 4C494345 49DFEF30 9F81488C
        304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4
        5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4


MacKey is
                              92EA 706A6FCE 4DD20D0B 918BC107


Mtag is
                                                        2762D05E
        EE45EB61 B2DEA75E C0F9A1A2 B93B1859 E74AEAD8 6CBBC6B2


KeyData is
                                            6EEE1FBC D5913742
        9C8B56B2 01D3D725 5180E8F1 1FF1DBB3 4C103100 28E02970
        8B050A83 44229341 09BD0362 8FC0BA70 8AA035DB B2D8C4F0
```

```
-----------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
                                                        4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9


Zs is
                                                        9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9


Ze is
                                                        59141E22
        76D41EDA D4E6D088 5C363DCF E91FCC0C 1726D11C FB3AA35B


Z is
                                            59141E22 76D41EDA
        D4E6D088 5C363DCF E91FCC0C 1726D11C FB3AA35B 9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            92EA 706A6FCE 4DD20D0B 918BC107 6EEE1FBC D5913742
        9C8B56B2 01D3D725 5180E8F1 1FF1DBB3 4C103100 28E02970
        8B050A83 44229341 09BD0362 8FC0BA70 8AA035DB B2D8C4F0


U2V
----------------
MacData is
                                                        4B435F32
        5F55414C 49434542 4F424259 49DFEF30 9F81488C 304CFF5A
        B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4 5762C4F6
        54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4 4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9
```

MacKey is
92EA 706A6FCE 4DD20D0B 918BC107

Mtag is
0954AFC0
2B5F3F3E 06FE2FF2 120D8695 C7D4BF77 7285B7CC F5691371

V2U

MacData is
4B435F32
5F56424F 42425941 4C494345 4327ABCA DC176812 553A2E13
F68080BE D1BC6A1A 4F6FBB12 345EC9F9 49DFEF30 9F81488C
304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4
5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4

MacKey is
92EA 706A6FCE 4DD20D0B 918BC107

Mtag is
CEFD1BF6
C74C966F 97B632FB 26E2129B 2AED8022 2CCE396E B95091C1

KeyData is
6EEE1FBC D5913742
9C8B56B2 01D3D725 5180E8F1 1FF1DBB3 4C103100 28E02970
8B050A83 44229341 09BD0362 8FC0BA70 8AA035DB B2D8C4F0

OnePassMQV(P-224)
---
dsU is
A273DD64
3AB8A64B 4B6E1FF9 C7ECF18E BC1F62DE 33450A9E 32E8A504

QsU_x is
FAD43A96
46721C46 52F13752 345FC2D5 25515A55 A170E685 314810E1

QsU_y is

```
                                                        E05BE902
        7238C138 7F7C5575 ED425324 32929EFB C2C37293 1253F3D2
```

dsV is

```
                                                        723A6551
        09089ED0 EDB4E630 72A82640 9F9C6204 635169F0 681F7514
```

QsV_x is

```
                                                        0898B1C4
        B9308496 45F2E605 00DA0492 0CB70272 3E4E13F6 64C99B0B
```

QsV_y is

```
                                                        0D91CF88
        A13435E4 D126DA64 352C75F2 B80C65F9 43D6F65A 6AC20F0B
```

deU is

```
                                                        B558EB6C
        288DA707 BBB4F8FB AE2AB9E9 CB62E3BC 5C7573E2 2E26D37F
```

QeU_x is

```
                                                        49DFEF30
        9F81488C 304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB
```

QeU_y is

```
                                                        4F2B5EE4
        5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4
```

---

no Key Confirmation
Z is

```
                                                        C94E2263
        B99BEB56 46CA803A B625A9F8 734BD00E C9533680 8DCC8732
```

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                62C37171 C44BE767
        4004DF4E B111664A 39C2E7AB 31C36CA0 0AA6996B CA481767
        09F68F9A B0C361C4 A34AACC4 ABE7A89B E78C547D 6829D25E


KeyData is
                                                62C37171 C44BE767
        4004DF4E B111664A 39C2E7AB 31C36CA0 0AA6996B CA481767
        09F68F9A B0C361C4 A34AACC4 ABE7A89B E78C547D 6829D25E




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                                                        4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9


Z is
                                                        C94E2263
        B99BEB56 46CA803A B625A9F8 734BD00E C9533680 8DCC8732


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            62C3 7171C44B E7674004 DF4EB111 664A39C2 E7AB31C3
        6CA00AA6 996BCA48 176709F6 8F9AB0C3 61C4A34A ACC4ABE7
        A89BE78C 547D6829 D25EAFD6 1602000B A871D962 B4BC59C5


MacData is
                                                        4B435F31
        5F55414C 49434542 4F424259 49DFEF30 9F81488C 304CFF5A
        B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4 5762C4F6
        54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4 4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9
```

```
MacKey is
                              62C3 7171C44B E7674004 DF4EB111


Mtag is
                                                      EBED799A
        91765BD7 A2D0CAE9 E7006E21 66058613 ED56873D 00EA3AF7


KeyData is
                                                664A39C2 E7AB31C3
        6CA00AA6 996BCA48 176709F6 8F9AB0C3 61C4A34A ACC4ABE7
        A89BE78C 547D6829 D25EAFD6 1602000B A871D962 B4BC59C5




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
                                                      4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9


Z is
                                                      C94E2263
        B99BEB56 46CA803A B625A9F8 734BD00E C9533680 8DCC8732


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            62C3 7171C44B E7674004 DF4EB111 664A39C2 E7AB31C3
        6CA00AA6 996BCA48 176709F6 8F9AB0C3 61C4A34A ACC4ABE7
        A89BE78C 547D6829 D25EAFD6 1602000B A871D962 B4BC59C5


MacData is
        4B435F31 5F56424F 42425941 4C494345 49DFEF30 9F81488C
        304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4
        5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4
```

```
MacKey is
                            62C3 7171C44B E7674004 DF4EB111


Mtag is
                                                        0D63208B
        C4ED7839 4C5FC832 DC7B51E2 F702CB05 FB297813 688336C0


KeyData is
                                               664A39C2 E7AB31C3
        6CA00AA6 996BCA48 176709F6 8F9AB0C3 61C4A34A ACC4ABE7
        A89BE78C 547D6829 D25EAFD6 1602000B A871D962 B4BC59C5




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
                                                        4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9


Z is
                                                        C94E2263
        B99BEB56 46CA803A B625A9F8 734BD00E C9533680 8DCC8732


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            62C3 7171C44B E7674004 DF4EB111 664A39C2 E7AB31C3
        6CA00AA6 996BCA48 176709F6 8F9AB0C3 61C4A34A ACC4ABE7
        A89BE78C 547D6829 D25EAFD6 1602000B A871D962 B4BC59C5


U2V
----------------
MacData is
                                                        4B435F32
        5F55414C 49434542 4F424259 49DFEF30 9F81488C 304CFF5A
        B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4 5762C4F6
```

```
        54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4 4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9


MacKey is
                            62C3 7171C44B E7674004 DF4EB111


Mtag is
                                                    B2E7A535
        1609EEFF B9DC6DDD 3A09FE05 F972F8E0 EEF1B4F8 9AF0834A


V2U
----------------
MacData is
                                                    4B435F32
        5F56424F 42425941 4C494345 4327ABCA DC176812 553A2E13
        F68080BE D1BC6A1A 4F6FBB12 345EC9F9 49DFEF30 9F81488C
        304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4
        5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4


MacKey is
                            62C3 7171C44B E7674004 DF4EB111


Mtag is
                                                    47F5EE5E
        51BA83C3 CB5F94BD D07742D1 38B37764 437F8923 874FCC9F


KeyData is
                                                664A39C2 E7AB31C3
        6CA00AA6 996BCA48 176709F6 8F9AB0C3 61C4A34A ACC4ABE7
        A89BE78C 547D6829 D25EAFD6 1602000B A871D962 B4BC59C5




OnePassDiffieHellmanCDH(P-224)
------------------------------------------------------------
dsV is
                                                    723A6551
        09089ED0 EDB4E630 72A82640 9F9C6204 635169F0 681F7514
```

```
QsV_x is
                                                        0898B1C4
        B9308496 45F2E605 00DA0492 0CB70272 3E4E13F6 64C99B0B


QsV_y is
                                                        0D91CF88
        A13435E4 D126DA64 352C75F2 B80C65F9 43D6F65A 6AC20F0B


deU is
                                                        B558EB6C
        288DA707 BBB4F8FB AE2AB9E9 CB62E3BC 5C7573E2 2E26D37F


QeU_x is
                                                        49DFEF30
        9F81488C 304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB


QeU_y is
                                                        4F2B5EE4
        5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4




-------------------------------------------------------------
no Key Confirmation
Z is
                                                        59141E22
        76D41EDA D4E6D088 5C363DCF E91FCC0C 1726D11C FB3AA35B


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                D9DAD952 FDA8BE9B
        1C3F0962 D5B21DC8 F87E85B1 D3521242 2E4458FC 1600B2D4
        5528EC66 ED6BB75E 8714B4EF BA31CD10 B0CEB5CF 74C480FA


KeyData is
```

```
                                                D9DAD952 FDA8BE9B
        1C3F0962 D5B21DC8 F87E85B1 D3521242 2E4458FC 1600B2D4
        5528EC66 ED6BB75E 8714B4EF BA31CD10 B0CEB5CF 74C480FA



-------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
                                                        59141E22
        76D41EDA D4E6D088 5C363DCF E91FCC0C 1726D11C FB3AA35B


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            D9DA D952FDA8 BE9B1C3F 0962D5B2 1DC8F87E 85B1D352
        12422E44 58FC1600 B2D45528 EC66ED6B B75E8714 B4EFBA31
        CD10B0CE B5CF74C4 80FAA515 716881E3 658C6202 B97D4E01


MacData is
        4B435F31 5F56424F 42425941 4C494345 49DFEF30 9F81488C
        304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4
        5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4


MacKey is
                               D9DA D952FDA8 BE9B1C3F 0962D5B2


Mtag is
                                                        AB02D5F4
        32638AA2 339EE0B5 07A31345 24EC7A1C 67A398A6 9D3BF981


KeyData is
                                                D9DA D952FDA8
        BE9B1C3F 0962D5B2 1DC8F87E 85B1D352 12422E44 58FC1600
        B2D45528 EC66ED6B B75E8714 B4EFBA31 CD10B0CE B5CF74C4
        80FAA515 716881E3 658C6202 B97D4E01
```

StaticUnifiedCDH(P-224)
---
dsU is
A273DD64
3AB8A64B 4B6E1FF9 C7ECF18E BC1F62DE 33450A9E 32E8A504

QsU_x is
FAD43A96
46721C46 52F13752 345FC2D5 25515A55 A170E685 314810E1

QsU_y is
E05BE902
7238C138 7F7C5575 ED425324 32929EFB C2C37293 1253F3D2

dsV is
723A6551
09089ED0 EDB4E630 72A82640 9F9C6204 635169F0 681F7514

QsV_x is
0898B1C4
B9308496 45F2E605 00DA0492 0CB70272 3E4E13F6 64C99B0B

QsV_y is
0D91CF88
A13435E4 D126DA64 352C75F2 B80C65F9 43D6F65A 6AC20F0B

---
no Key Confirmation
NonceU is
4327ABCA
DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9

Z is
9F18FF54
F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9

```
OtherInfo is
                                                    1234 56789ABC
        DEF0414C 49434531 3233E000 4327ABCA DC176812 553A2E13
        F68080BE D1BC6A1A 4F6FBB12 345EC9F9 424F4242 59343536


DerivedKeyMaterial is
                                                  3A15B245 C1EA216C
        5FEB3768 EABFB0F1 144477D4 AB41AC6C C6E73717 08B21A9B
        FC99DEBB 82AD4852 68037AC2 1FEF9BA5 54283FE3 6114230C


KeyData is
                                                  3A15B245 C1EA216C
        5FEB3768 EABFB0F1 144477D4 AB41AC6C C6E73717 08B21A9B
        FC99DEBB 82AD4852 68037AC2 1FEF9BA5 54283FE3 6114230C




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceU is
                                                    4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9


NonceV is
                                                    A863E43A
        B0C1163A 741A10AE F27BD6BE 6E8E3E45 0B8BCE01 DF0DA8B2


Z is
                                                    9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9


OtherInfo is
                                                    1234 56789ABC
        DEF0414C 49434531 3233E000 4327ABCA DC176812 553A2E13
        F68080BE D1BC6A1A 4F6FBB12 345EC9F9 424F4242 59343536


DerivedKeyMaterial is
            3A15 B245C1EA 216C5FEB 3768EABF B0F11444 77D4AB41
```

```
        AC6CC6E7 371708B2 1A9BFC99 DEBB82AD 48526803 7AC21FEF
        9BA55428 3FE36114 230C2C72 8DBDB69A 34153BF1 BAA71580


MacData is
        4B435F31 5F55414C 49434542 4F424259 4327ABCA DC176812
        553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9 A863E43A
        B0C1163A 741A10AE F27BD6BE 6E8E3E45 0B8BCE01 DF0DA8B2


MacKey is
                            3A15 B245C1EA 216C5FEB 3768EABF


Mtag is
                                                    78EA5BF9
        DC24A78E A6D94FA1 46A8BC6F 5E29B63F 6B85695C 27425489


KeyData is
                                               B0F11444 77D4AB41
        AC6CC6E7 371708B2 1A9BFC99 DEBB82AD 48526803 7AC21FEF
        9BA55428 3FE36114 230C2C72 8DBDB69A 34153BF1 BAA71580




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceV is
                                                    A863E43A
        B0C1163A 741A10AE F27BD6BE 6E8E3E45 0B8BCE01 DF0DA8B2


NonceU is
                                                    4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9


Z is
                                                    9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9


OtherInfo is
                                                1234 56789ABC
```

```
        DEF0414C 49434531 3233E000 4327ABCA DC176812 553A2E13
        F68080BE D1BC6A1A 4F6FBB12 345EC9F9 424F4242 59343536


DerivedKeyMaterial is
            3A15 B245C1EA 216C5FEB 3768EABF B0F11444 77D4AB41
        AC6CC6E7 371708B2 1A9BFC99 DEBB82AD 48526803 7AC21FEF
        9BA55428 3FE36114 230C2C72 8DBDB69A 34153BF1 BAA71580


MacData is
                 4B435F31 5F56424F 42425941 4C494345 4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9


MacKey is
                             3A15 B245C1EA 216C5FEB 3768EABF


Mtag is
                                                    8D3DCDAF
        B2E7F89B 2ACFC757 828BC46C E708C8AC 0D59DE08 95779651


KeyData is
                                               B0F11444 77D4AB41
        AC6CC6E7 371708B2 1A9BFC99 DEBB82AD 48526803 7AC21FEF
        9BA55428 3FE36114 230C2C72 8DBDB69A 34153BF1 BAA71580




-------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
NonceU is
                                                    4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9


NonceV is
                                                    A863E43A
        B0C1163A 741A10AE F27BD6BE 6E8E3E45 0B8BCE01 DF0DA8B2


Z is
```

                                                        9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9

OtherInfo is
                                                    1234 56789ABC
        DEF0414C 49434531 3233E000 4327ABCA DC176812 553A2E13
        F68080BE D1BC6A1A 4F6FBB12 345EC9F9 424F4242 59343536

DerivedKeyMaterial is
            3A15 B245C1EA 216C5FEB 3768EABF B0F11444 77D4AB41
        AC6CC6E7 371708B2 1A9BFC99 DEBB82AD 48526803 7AC21FEF
        9BA55428 3FE36114 230C2C72 8DBDB69A 34153BF1 BAA71580

U2V

MacData is
        4B435F32 5F55414C 49434542 4F424259 4327ABCA DC176812
        553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9 A863E43A
        B0C1163A 741A10AE F27BD6BE 6E8E3E45 0B8BCE01 DF0DA8B2

MacKey is
                            3A15 B245C1EA 216C5FEB 3768EABF

Mtag is
                                                        701F901A
        59DB352A 63F83B7A 4AB75B70 E1676941 38F2A82E D877DA3E

V2U

MacData is
        4B435F32 5F56424F 42425941 4C494345 A863E43A B0C1163A
        741A10AE F27BD6BE 6E8E3E45 0B8BCE01 DF0DA8B2 4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9

MacKey is
                            3A15 B245C1EA 216C5FEB 3768EABF

Mtag is

```
                                                        CDF6A578
        6125F911 209D68F0 F58F16F5 ACEED698 A21394AE 4DA3C33D


KeyData is
                                               B0F11444 77D4AB41
        AC6CC6E7 371708B2 1A9BFC99 DEBB82AD 48526803 7AC21FEF
        9BA55428 3FE36114 230C2C72 8DBDB69A 34153BF1 BAA71580
```

FullUnifiedCDH(P-256)
---
dsU is
5DCDF2A3 3538D7CF
93A3680D 4CB4E86A 6814DA67 AC5D8323 EDBAAA59 FAAA2DE4

QsU_x is
E960C4EA 199B35D5
4CA122BB D85A61A3 0015FB9C 1FA43BE5 C04B4642 7D5206AB

QsU_y is
4EF04F38 77329ACF
60A13454 CC169266 6497DD57 B8705B0F C9459649 7E433532

dsV is
8FED7843 1D82558D
9006C3DE B06AB58D 9DCCC971 06875C67 25D5F166 255BA90A

QsV_x is
1B1631C5 DC76D378
A914C967 29D0A594 D54B4F58 845B1D4A 4B6BE739 CA4A18EA

QsV_y is
4F85E4C9 26EE5323
90AA7CD4 14943537 25E6E804 714AA69D 67072F65 DB625E07

deU is
81426414 5F2F56F2
E96A8E33 7A128499 3FAF432A 5ABCE59E 867B7291 D507A3AF

QeU_x is
2AF502F3 BE8952F2
C9B5A8D4 160D09E9 7165BE50 BC42AE4A 5E8D3B4B A83AEB15

QeU_y is
EB0FAF4C A986C4D3

```
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85


deV is
                                                2CE1788E C197E096
        DB95A200 CC0AB26A 19CE6BCC AD562B8E EE1B5937 61CF7F41


QeV_x is
                                                B120DE4A A3649279
        5346E8DE 6C2C8646 AE06AAEA 279FA775 B3AB0715 F6CE51B0


QeV_y is
                                                9F1B7EEC E20D7B5E
        D8EC685F A3F071D8 37270270 92A84113 85C34DDE 5708B2B6




------------------------------------------------------------
no Key Confirmation
Zs is
                                                227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


Ze is
                                                DD0F5396 219D1EA3
        93310412 D19A08F1 F5811E9D C8EC8EEA 7F80D21C 820C2788


Z is
                        DD0F5396 219D1EA3 93310412 D19A08F1
        F5811E9D C8EC8EEA 7F80D21C 820C2788 227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                        C08B3DE2 4F1A381E 7A5675A2 A6523B08
        F354605E EE46B9F3 9EADB1E9 7534416D 98B43CAE 8AB04AFD
        53DEB37F 44022352 C3FBDE1E 2F2CEC53 1CFC324F DD0FCCA6
```

```
KeyData is
                          C08B3DE2 4F1A381E 7A5675A2 A6523B08
        F354605E EE46B9F3 9EADB1E9 7534416D 98B43CAE 8AB04AFD
        53DEB37F 44022352 C3FBDE1E 2F2CEC53 1CFC324F DD0FCCA6



------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Zs is
                                                227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


Ze is
                                                DD0F5396 219D1EA3
        93310412 D19A08F1 F5811E9D C8EC8EEA 7F80D21C 820C2788


Z is
                          DD0F5396 219D1EA3 93310412 D19A08F1
        F5811E9D C8EC8EEA 7F80D21C 820C2788 227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                C08B3DE2 4F1A381E
        7A5675A2 A6523B08 F354605E EE46B9F3 9EADB1E9 7534416D
        98B43CAE 8AB04AFD 53DEB37F 44022352 C3FBDE1E 2F2CEC53
        1CFC324F DD0FCCA6 9B778342 70D4ED54 6720F5EF 269C95C2


MacData is
        4B435F31 5F55414C 49434542 4F424259 2AF502F3 BE8952F2
        C9B5A8D4 160D09E9 7165BE50 BC42AE4A 5E8D3B4B A83AEB15
        EB0FAF4C A986C4D3 8681A0F9 872D79D5 6795BD4B FF6E6DE3
        C0F5015E CE5EFD85 B120DE4A A3649279 5346E8DE 6C2C8646
        AE06AAEA 279FA775 B3AB0715 F6CE51B0 9F1B7EEC E20D7B5E
        D8EC685F A3F071D8 37270270 92A84113 85C34DDE 5708B2B6
```

MacKey is
                        C08B3DE2 4F1A381E 7A5675A2 A6523B08

Mtag is
                                            5CFD5CC4 D489476E
        65EE2E20 DF948DF9 A6B311B7 270CBEA1 9E309760 ECF2F4E4

KeyData is
                        F354605E EE46B9F3 9EADB1E9 7534416D
        98B43CAE 8AB04AFD 53DEB37F 44022352 C3FBDE1E 2F2CEC53
        1CFC324F DD0FCCA6 9B778342 70D4ED54 6720F5EF 269C95C2

Scheme Responder, Key Confirmation Provider: V to U
Zs is
                                            227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F

Ze is
                                            DD0F5396 219D1EA3
        93310412 D19A08F1 F5811E9D C8EC8EEA 7F80D21C 820C2788

Z is
                        DD0F5396 219D1EA3 93310412 D19A08F1
        F5811E9D C8EC8EEA 7F80D21C 820C2788 227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                                            C08B3DE2 4F1A381E
        7A5675A2 A6523B08 F354605E EE46B9F3 9EADB1E9 7534416D
        98B43CAE 8AB04AFD 53DEB37F 44022352 C3FBDE1E 2F2CEC53
        1CFC324F DD0FCCA6 9B778342 70D4ED54 6720F5EF 269C95C2

```
MacData is
        4B435F31 5F56424F 42425941 4C494345 B120DE4A A3649279
        5346E8DE 6C2C8646 AE06AAEA 279FA775 B3AB0715 F6CE51B0
        9F1B7EEC E20D7B5E D8EC685F A3F071D8 37270270 92A84113
        85C34DDE 5708B2B6 2AF502F3 BE8952F2 C9B5A8D4 160D09E9
        7165BE50 BC42AE4A 5E8D3B4B A83AEB15 EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85


MacKey is
                         C08B3DE2 4F1A381E 7A5675A2 A6523B08


Mtag is
                                            206CBE5D 40AAAC1E
        678ED3F7 C248F4BF D3B1AE0E 60B3089A C179AAB7 B1D4FF55


KeyData is
                         F354605E EE46B9F3 9EADB1E9 7534416D
        98B43CAE 8AB04AFD 53DEB37F 44022352 C3FBDE1E 2F2CEC53
        1CFC324F DD0FCCA6 9B778342 70D4ED54 6720F5EF 269C95C2




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
Zs is
                                            227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


Ze is
                                            DD0F5396 219D1EA3
        93310412 D19A08F1 F5811E9D C8EC8EEA 7F80D21C 820C2788


Z is
                         DD0F5396 219D1EA3 93310412 D19A08F1
        F5811E9D C8EC8EEA 7F80D21C 820C2788 227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F
```

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                            C08B3DE2 4F1A381E
        7A5675A2 A6523B08 F354605E EE46B9F3 9EADB1E9 7534416D
        98B43CAE 8AB04AFD 53DEB37F 44022352 C3FBDE1E 2F2CEC53
        1CFC324F DD0FCCA6 9B778342 70D4ED54 6720F5EF 269C95C2


U2V
----------------
MacData is
        4B435F32 5F55414C 49434542 4F424259 2AF502F3 BE8952F2
        C9B5A8D4 160D09E9 7165BE50 BC42AE4A 5E8D3B4B A83AEB15
        EB0FAF4C A986C4D3 8681A0F9 872D79D5 6795BD4B FF6E6DE3
        C0F5015E CE5EFD85 B120DE4A A3649279 5346E8DE 6C2C8646
        AE06AAEA 279FA775 B3AB0715 F6CE51B0 9F1B7EEC E20D7B5E
        D8EC685F A3F071D8 37270270 92A84113 85C34DDE 5708B2B6


MacKey is
                          C08B3DE2 4F1A381E 7A5675A2 A6523B08


Mtag is
                                            91C619A8 7851D80A
        1142688B 0CDDC3A1 A2B20147 CA2C0ECF 04265EAF 8448DA3B


V2U
----------------
MacData is
        4B435F32 5F56424F 42425941 4C494345 B120DE4A A3649279
        5346E8DE 6C2C8646 AE06AAEA 279FA775 B3AB0715 F6CE51B0
        9F1B7EEC E20D7B5E D8EC685F A3F071D8 37270270 92A84113
        85C34DDE 5708B2B6 2AF502F3 BE8952F2 C9B5A8D4 160D09E9
        7165BE50 BC42AE4A 5E8D3B4B A83AEB15 EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85


MacKey is
                          C08B3DE2 4F1A381E 7A5675A2 A6523B08
```

```
Mtag is
                                                F3267D2F E5CDBCEF
        E763E96E C3974832 1B32B0EF 737D97A2 74DE6502 88107E41


KeyData is
                            F354605E EE46B9F3 9EADB1E9 7534416D
        98B43CAE 8AB04AFD 53DEB37F 44022352 C3FBDE1E 2F2CEC53
        1CFC324F DD0FCCA6 9B778342 70D4ED54 6720F5EF 269C95C2




FullMQV(P-256)
------------------------------------------------------------
dsU is
                                                5DCDF2A3 3538D7CF
        93A3680D 4CB4E86A 6814DA67 AC5D8323 EDBAAA59 FAAA2DE4


QsU_x is
                                                E960C4EA 199B35D5
        4CA122BB D85A61A3 0015FB9C 1FA43BE5 C04B4642 7D5206AB


QsU_y is
                                                4EF04F38 77329ACF
        60A13454 CC169266 6497DD57 B8705B0F C9459649 7E433532


dsV is
                                                8FED7843 1D82558D
        9006C3DE B06AB58D 9DCCC971 06875C67 25D5F166 255BA90A


QsV_x is
                                                1B1631C5 DC76D378
        A914C967 29D0A594 D54B4F58 845B1D4A 4B6BE739 CA4A18EA


QsV_y is
                                                4F85E4C9 26EE5323
        90AA7CD4 14943537 25E6E804 714AA69D 67072F65 DB625E07


deU is
```

```
                                                81426414 5F2F56F2
        E96A8E33 7A128499 3FAF432A 5ABCE59E 867B7291 D507A3AF


QeU_x is
                                                2AF502F3 BE8952F2
        C9B5A8D4 160D09E9 7165BE50 BC42AE4A 5E8D3B4B A83AEB15


QeU_y is
                                                EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85


deV is
                                                2CE1788E C197E096
        DB95A200 CC0AB26A 19CE6BCC AD562B8E EE1B5937 61CF7F41


QeV_x is
                                                B120DE4A A3649279
        5346E8DE 6C2C8646 AE06AAEA 279FA775 B3AB0715 F6CE51B0


QeV_y is
                                                9F1B7EEC E20D7B5E
        D8EC685F A3F071D8 37270270 92A84113 85C34DDE 5708B2B6




------------------------------------------------------------
no Key Confirmation
Z is
                                                83050B73 1021FDBD
        B13FFE9F DE0373A8 C917C6FA 8106636C 1E1F7D15 64566219


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                            D71E0F55 D4EF4431 816EE299 715EA93D
        D116BDC8 803D66EA FEF37A07 5DB6A2A4 6AEF2BC5 D38A77EE
        40D34283 58580E87 99A4F70A E7353D69 AD2C964A 113ABFDD
```

KeyData is
                        D71E0F55 D4EF4431 816EE299 715EA93D
        D116BDC8 803D66EA FEF37A07 5DB6A2A4 6AEF2BC5 D38A77EE
        40D34283 58580E87 99A4F70A E7353D69 AD2C964A 113ABFDD

Scheme Initiator, Key Confirmation Provider: U to V
Z is
                                                83050B73 1021FDBD
        B13FFE9F DE0373A8 C917C6FA 8106636C 1E1F7D15 64566219

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                                                D71E0F55 D4EF4431
        816EE299 715EA93D D116BDC8 803D66EA FEF37A07 5DB6A2A4
        6AEF2BC5 D38A77EE 40D34283 58580E87 99A4F70A E7353D69
        AD2C964A 113ABFDD 8129D8D2 3847448A 934B832D E3DFCFA8

MacData is
        4B435F31 5F55414C 49434542 4F424259 2AF502F3 BE8952F2
        C9B5A8D4 160D09E9 7165BE50 BC42AE4A 5E8D3B4B A83AEB15
        EB0FAF4C A986C4D3 8681A0F9 872D79D5 6795BD4B FF6E6DE3
        C0F5015E CE5EFD85 B120DE4A A3649279 5346E8DE 6C2C8646
        AE06AAEA 279FA775 B3AB0715 F6CE51B0 9F1B7EEC E20D7B5E
        D8EC685F A3F071D8 37270270 92A84113 85C34DDE 5708B2B6

MacKey is
                        D71E0F55 D4EF4431 816EE299 715EA93D

Mtag is
                                                19B74E52 B5966E9C
        49A31324 36F17A7F 51EF40D0 15F677B7 B8F3B7BB 455CE8D0

KeyData is
                        D116BDC8 803D66EA FEF37A07 5DB6A2A4
        6AEF2BC5 D38A77EE 40D34283 58580E87 99A4F70A E7353D69
        AD2C964A 113ABFDD 8129D8D2 3847448A 934B832D E3DFCFA8

Scheme Responder, Key Confirmation Provider: V to U
Z is
                                                83050B73 1021FDBD
        B13FFE9F DE0373A8 C917C6FA 8106636C 1E1F7D15 64566219

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                                                D71E0F55 D4EF4431
        816EE299 715EA93D D116BDC8 803D66EA FEF37A07 5DB6A2A4
        6AEF2BC5 D38A77EE 40D34283 58580E87 99A4F70A E7353D69
        AD2C964A 113ABFDD 8129D8D2 3847448A 934B832D E3DFCFA8

MacData is
        4B435F31 5F56424F 42425941 4C494345 B120DE4A A3649279
        5346E8DE 6C2C8646 AE06AAEA 279FA775 B3AB0715 F6CE51B0
        9F1B7EEC E20D7B5E D8EC685F A3F071D8 37270270 92A84113
        85C34DDE 5708B2B6 2AF502F3 BE8952F2 C9B5A8D4 160D09E9
        7165BE50 BC42AE4A 5E8D3B4B A83AEB15 EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85

MacKey is
                        D71E0F55 D4EF4431 816EE299 715EA93D

Mtag is
                                                D638EDCF F42CAE22
        BDF90E84 FA3E9CE2 55CC8FCD CA176B8B CC42A5F0 7B3E77B0

KeyData is
                        D116BDC8 803D66EA FEF37A07 5DB6A2A4

```
        6AEF2BC5 D38A77EE 40D34283 58580E87 99A4F70A E7353D69
        AD2C964A 113ABFDD 8129D8D2 3847448A 934B832D E3DFCFA8



-------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
Z is
                                                83050B73 1021FDBD
        B13FFE9F DE0373A8 C917C6FA 8106636C 1E1F7D15 64566219


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                D71E0F55 D4EF4431
        816EE299 715EA93D D116BDC8 803D66EA FEF37A07 5DB6A2A4
        6AEF2BC5 D38A77EE 40D34283 58580E87 99A4F70A E7353D69
        AD2C964A 113ABFDD 8129D8D2 3847448A 934B832D E3DFCFA8


U2V
----------------
MacData is
        4B435F32 5F55414C 49434542 4F424259 2AF502F3 BE8952F2
        C9B5A8D4 160D09E9 7165BE50 BC42AE4A 5E8D3B4B A83AEB15
        EB0FAF4C A986C4D3 8681A0F9 872D79D5 6795BD4B FF6E6DE3
        C0F5015E CE5EFD85 B120DE4A A3649279 5346E8DE 6C2C8646
        AE06AAEA 279FA775 B3AB0715 F6CE51B0 9F1B7EEC E20D7B5E
        D8EC685F A3F071D8 37270270 92A84113 85C34DDE 5708B2B6


MacKey is
                          D71E0F55 D4EF4431 816EE299 715EA93D


Mtag is
                                                37690854 0BECD752
        958AB6CD 70AEF7DE 21091A9C C4B51B1F 64FBE347 8CBE0C84


V2U
```

```
----------------
MacData is
        4B435F32 5F56424F 42425941 4C494345 B120DE4A A3649279
        5346E8DE 6C2C8646 AE06AAEA 279FA775 B3AB0715 F6CE51B0
        9F1B7EEC E20D7B5E D8EC685F A3F071D8 37270270 92A84113
        85C34DDE 5708B2B6 2AF502F3 BE8952F2 C9B5A8D4 160D09E9
        7165BE50 BC42AE4A 5E8D3B4B A83AEB15 EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85


MacKey is
                        D71E0F55 D4EF4431 816EE299 715EA93D


Mtag is
                                          8ACB634F 83232041
        0F1AE1DA 4359D31B E87D3E62 2791D904 0B3A3687 948A24EE


KeyData is
                        D116BDC8 803D66EA FEF37A07 5DB6A2A4
        6AEF2BC5 D38A77EE 40D34283 58580E87 99A4F70A E7353D69
        AD2C964A 113ABFDD 8129D8D2 3847448A 934B832D E3DFCFA8




EphemeralUnifiedCDH(P-256)
------------------------------------------------------------
deU is
                                          81426414 5F2F56F2
        E96A8E33 7A128499 3FAF432A 5ABCE59E 867B7291 D507A3AF


QeU_x is
                                          2AF502F3 BE8952F2
        C9B5A8D4 160D09E9 7165BE50 BC42AE4A 5E8D3B4B A83AEB15


QeU_y is
                                          EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85


deV is
                                          2CE1788E C197E096
```

```
        DB95A200 CC0AB26A 19CE6BCC AD562B8E EE1B5937 61CF7F41


QeV_x is
                                                B120DE4A A3649279
        5346E8DE 6C2C8646 AE06AAEA 279FA775 B3AB0715 F6CE51B0


QeV_y is
                                                9F1B7EEC E20D7B5E
        D8EC685F A3F071D8 37270270 92A84113 85C34DDE 5708B2B6




------------------------------------------------------------
no Key Confirmation
Z is
                                                DD0F5396 219D1EA3
        93310412 D19A08F1 F5811E9D C8EC8EEA 7F80D21C 820C2788


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         4C664A9B CA73D981 9538F659 B4B675C7
        2FB95AC2 F86527D9 8254F85E 1041CBFA 386EEA63 B4DA8803
        B31383B5 44D33A0B C781F7C2 F66A8CF4 1DE148E2 D3328173


KeyData is
                         4C664A9B CA73D981 9538F659 B4B675C7
        2FB95AC2 F86527D9 8254F85E 1041CBFA 386EEA63 B4DA8803
        B31383B5 44D33A0B C781F7C2 F66A8CF4 1DE148E2 D3328173




OnePassUnifiedCDH(P-256)
------------------------------------------------------------
dsU is
                                                5DCDF2A3 3538D7CF
        93A3680D 4CB4E86A 6814DA67 AC5D8323 EDBAAA59 FAAA2DE4
```

QsU_x is
                                                E960C4EA 199B35D5
        4CA122BB D85A61A3 0015FB9C 1FA43BE5 C04B4642 7D5206AB

QsU_y is
                                                4EF04F38 77329ACF
        60A13454 CC169266 6497DD57 B8705B0F C9459649 7E433532

dsV is
                                                8FED7843 1D82558D
        9006C3DE B06AB58D 9DCCC971 06875C67 25D5F166 255BA90A

QsV_x is
                                                1B1631C5 DC76D378
        A914C967 29D0A594 D54B4F58 845B1D4A 4B6BE739 CA4A18EA

QsV_y is
                                                4F85E4C9 26EE5323
        90AA7CD4 14943537 25E6E804 714AA69D 67072F65 DB625E07

deU is
                                                81426414 5F2F56F2
        E96A8E33 7A128499 3FAF432A 5ABCE59E 867B7291 D507A3AF

QeU_x is
                                                2AF502F3 BE8952F2
        C9B5A8D4 160D09E9 7165BE50 BC42AE4A 5E8D3B4B A83AEB15

QeU_y is
                                                EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85

----
no Key Confirmation
Zs is

```
                                                227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


Ze is
                                                F9C34B92 ACEA12A0
        C50760E5 9D06C01F 72A0A5CD 8B1BFDD7 3DC8109A 8F8151B3


Z is
                         F9C34B92 ACEA12A0 C50760E5 9D06C01F
        72A0A5CD 8B1BFDD7 3DC8109A 8F8151B3 227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         C9FE943A B7241197 98158A10 E50DF332
        4593317C C9CBE7CD D4F99D11 B45E0C3B BAA16916 9C6D949A
        87450F4D 83B67C54 ADB69BEC D6271E83 5E22A058 7919484F


KeyData is
                         C9FE943A B7241197 98158A10 E50DF332
        4593317C C9CBE7CD D4F99D11 B45E0C3B BAA16916 9C6D949A
        87450F4D 83B67C54 ADB69BEC D6271E83 5E22A058 7919484F




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                                                817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


Zs is
                                                227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


Ze is
```

```
                                            F9C34B92 ACEA12A0
        C50760E5 9D06C01F 72A0A5CD 8B1BFDD7 3DC8109A 8F8151B3


Z is
                        F9C34B92 ACEA12A0 C50760E5 9D06C01F
        72A0A5CD 8B1BFDD7 3DC8109A 8F8151B3 227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                            C9FE943A B7241197
        98158A10 E50DF332 4593317C C9CBE7CD D4F99D11 B45E0C3B
        BAA16916 9C6D949A 87450F4D 83B67C54 ADB69BEC D6271E83
        5E22A058 7919484F FD288D71 BB78F910 B980487C 0631603B


MacData is
                        4B435F31 5F55414C 49434542 4F424259
        2AF502F3 BE8952F2 C9B5A8D4 160D09E9 7165BE50 BC42AE4A
        5E8D3B4B A83AEB15 EB0FAF4C A986C4D3 8681A0F9 872D79D5
        6795BD4B FF6E6DE3 C0F5015E CE5EFD85 817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


MacKey is
                        C9FE943A B7241197 98158A10 E50DF332


Mtag is
                                            12DEF174 D12ADC8A
        2EAFB7B4 90B9CB10 F7514FDE 21EA2A5C E856EA63 D78E94C3


KeyData is
                        4593317C C9CBE7CD D4F99D11 B45E0C3B
        BAA16916 9C6D949A 87450F4D 83B67C54 ADB69BEC D6271E83
        5E22A058 7919484F FD288D71 BB78F910 B980487C 0631603B
```

```
------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
                                                817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


Zs is
                                                227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


Ze is
                                                F9C34B92 ACEA12A0
        C50760E5 9D06C01F 72A0A5CD 8B1BFDD7 3DC8109A 8F8151B3


Z is
                        F9C34B92 ACEA12A0 C50760E5 9D06C01F
        72A0A5CD 8B1BFDD7 3DC8109A 8F8151B3 227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                C9FE943A B7241197
        98158A10 E50DF332 4593317C C9CBE7CD D4F99D11 B45E0C3B
        BAA16916 9C6D949A 87450F4D 83B67C54 ADB69BEC D6271E83
        5E22A058 7919484F FD288D71 BB78F910 B980487C 0631603B


MacData is
                                                4B435F31 5F56424F
        42425941 4C494345 2AF502F3 BE8952F2 C9B5A8D4 160D09E9
        7165BE50 BC42AE4A 5E8D3B4B A83AEB15 EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85


MacKey is
                        C9FE943A B7241197 98158A10 E50DF332


Mtag is
```

```
                                                50DDD00D 351C9953
        9380B9E5 06005963 2E48FC1E 4E392E69 B7A20E0D 25078FAE


KeyData is
                            4593317C C9CBE7CD D4F99D11 B45E0C3B
        BAA16916 9C6D949A 87450F4D 83B67C54 ADB69BEC D6271E83
        5E22A058 7919484F FD288D71 BB78F910 B980487C 0631603B




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
                                                817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


Zs is
                                                227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


Ze is
                                                F9C34B92 ACEA12A0
        C50760E5 9D06C01F 72A0A5CD 8B1BFDD7 3DC8109A 8F8151B3


Z is
                            F9C34B92 ACEA12A0 C50760E5 9D06C01F
        72A0A5CD 8B1BFDD7 3DC8109A 8F8151B3 227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                C9FE943A B7241197
        98158A10 E50DF332 4593317C C9CBE7CD D4F99D11 B45E0C3B
        BAA16916 9C6D949A 87450F4D 83B67C54 ADB69BEC D6271E83
        5E22A058 7919484F FD288D71 BB78F910 B980487C 0631603B
```

```
U2V
----------------
MacData is
                        4B435F32 5F55414C 49434542 4F424259
        2AF502F3 BE8952F2 C9B5A8D4 160D09E9 7165BE50 BC42AE4A
        5E8D3B4B A83AEB15 EB0FAF4C A986C4D3 8681A0F9 872D79D5
        6795BD4B FF6E6DE3 C0F5015E CE5EFD85 817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


MacKey is
                        C9FE943A B7241197 98158A10 E50DF332


Mtag is
                                            41F50954 02FAA2D8
        17F0F865 03B5285D E6088DEC 4875230A 78EEE770 4CB4D96B


V2U
----------------
MacData is
                        4B435F32 5F56424F 42425941 4C494345
        817807C9 E8826EE1 CFB2F373 26D32195 585BD75A 5140460F
        D9BC7139 82B4D7DA 2AF502F3 BE8952F2 C9B5A8D4 160D09E9
        7165BE50 BC42AE4A 5E8D3B4B A83AEB15 EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85


MacKey is
                        C9FE943A B7241197 98158A10 E50DF332


Mtag is
                                            8C200B72 CF72375D
        30702D0B B9E3A398 1D4EA7EF F558928F 2F2F8DE5 52E016C3


KeyData is
                        4593317C C9CBE7CD D4F99D11 B45E0C3B
        BAA16916 9C6D949A 87450F4D 83B67C54 ADB69BEC D6271E83
        5E22A058 7919484F FD288D71 BB78F910 B980487C 0631603B
```

OnePassMQV(P-256)
---

dsU is
5DCDF2A3 3538D7CF
93A3680D 4CB4E86A 6814DA67 AC5D8323 EDBAAA59 FAAA2DE4

QsU_x is
E960C4EA 199B35D5
4CA122BB D85A61A3 0015FB9C 1FA43BE5 C04B4642 7D5206AB

QsU_y is
4EF04F38 77329ACF
60A13454 CC169266 6497DD57 B8705B0F C9459649 7E433532

dsV is
8FED7843 1D82558D
9006C3DE B06AB58D 9DCCC971 06875C67 25D5F166 255BA90A

QsV_x is
1B1631C5 DC76D378
A914C967 29D0A594 D54B4F58 845B1D4A 4B6BE739 CA4A18EA

QsV_y is
4F85E4C9 26EE5323
90AA7CD4 14943537 25E6E804 714AA69D 67072F65 DB625E07

deU is
81426414 5F2F56F2
E96A8E33 7A128499 3FAF432A 5ABCE59E 867B7291 D507A3AF

QeU_x is
2AF502F3 BE8952F2
C9B5A8D4 160D09E9 7165BE50 BC42AE4A 5E8D3B4B A83AEB15

QeU_y is
EB0FAF4C A986C4D3
8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85

```
------------------------------------------------------------
no Key Confirmation
Z is
                                            D67DA92B 55FCB46A
        A03E23E5 42F4184C E93C534D 4BE9E9AC F3327355 3DD47A5B


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         139A77DD 97F7C9A3 D14F30B7 C27A0330
        2F392FED 08FC8839 9FF07B8B D2E34554 08F20BBC 72322228
        50F5C90A 14F52346 23C4D985 6F8C86A6 AACD2879 C4B5A626


KeyData is
                         139A77DD 97F7C9A3 D14F30B7 C27A0330
        2F392FED 08FC8839 9FF07B8B D2E34554 08F20BBC 72322228
        50F5C90A 14F52346 23C4D985 6F8C86A6 AACD2879 C4B5A626




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                                            817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


Z is
                                            D67DA92B 55FCB46A
        A03E23E5 42F4184C E93C534D 4BE9E9AC F3327355 3DD47A5B


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                            139A77DD 97F7C9A3
```

```
        D14F30B7 C27A0330 2F392FED 08FC8839 9FF07B8B D2E34554
        08F20BBC 72322228 50F5C90A 14F52346 23C4D985 6F8C86A6
        AACD2879 C4B5A626 4104CC9E A0DEF14F 11345D1F 0174389C


MacData is
                         4B435F31 5F55414C 49434542 4F424259
        2AF502F3 BE8952F2 C9B5A8D4 160D09E9 7165BE50 BC42AE4A
        5E8D3B4B A83AEB15 EB0FAF4C A986C4D3 8681A0F9 872D79D5
        6795BD4B FF6E6DE3 C0F5015E CE5EFD85 817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


MacKey is
                         139A77DD 97F7C9A3 D14F30B7 C27A0330


Mtag is
                                           8C795D0E 97C8EF29
        C7A63AFE B581D6E7 53A75551 61255355 F26F35B2 56604CDD


KeyData is
                         2F392FED 08FC8839 9FF07B8B D2E34554
        08F20BBC 72322228 50F5C90A 14F52346 23C4D985 6F8C86A6
        AACD2879 C4B5A626 4104CC9E A0DEF14F 11345D1F 0174389C




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
                                           817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


Z is
                                           D67DA92B 55FCB46A
        A03E23E5 42F4184C E93C534D 4BE9E9AC F3327355 3DD47A5B


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536
```

```
DerivedKeyMaterial is
                                                139A77DD 97F7C9A3
        D14F30B7 C27A0330 2F392FED 08FC8839 9FF07B8B D2E34554
        08F20BBC 72322228 50F5C90A 14F52346 23C4D985 6F8C86A6
        AACD2879 C4B5A626 4104CC9E A0DEF14F 11345D1F 0174389C


MacData is
                                                4B435F31 5F56424F
        42425941 4C494345 2AF502F3 BE8952F2 C9B5A8D4 160D09E9
        7165BE50 BC42AE4A 5E8D3B4B A83AEB15 EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85


MacKey is
                           139A77DD 97F7C9A3 D14F30B7 C27A0330


Mtag is
                                                518F4660 3D6E107A
        1C21EFDB 8D52028B FF32400A A8BF8763 876DEDFE 410003A3


KeyData is
                           2F392FED 08FC8839 9FF07B8B D2E34554
        08F20BBC 72322228 50F5C90A 14F52346 23C4D985 6F8C86A6
        AACD2879 C4B5A626 4104CC9E A0DEF14F 11345D1F 0174389C




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
                                                817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


Z is
                                                D67DA92B 55FCB46A
        A03E23E5 42F4184C E93C534D 4BE9E9AC F3327355 3DD47A5B


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536
```

```
DerivedKeyMaterial is
                                                139A77DD 97F7C9A3
        D14F30B7 C27A0330 2F392FED 08FC8839 9FF07B8B D2E34554
        08F20BBC 72322228 50F5C90A 14F52346 23C4D985 6F8C86A6
        AACD2879 C4B5A626 4104CC9E A0DEF14F 11345D1F 0174389C


U2V
----------------
MacData is
                        4B435F32 5F55414C 49434542 4F424259
        2AF502F3 BE8952F2 C9B5A8D4 160D09E9 7165BE50 BC42AE4A
        5E8D3B4B A83AEB15 EB0FAF4C A986C4D3 8681A0F9 872D79D5
        6795BD4B FF6E6DE3 C0F5015E CE5EFD85 817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


MacKey is
                        139A77DD 97F7C9A3 D14F30B7 C27A0330


Mtag is
                                                9C14D68B A0421C8D
        70863331 AE7A6571 8575724C 49E6D27F 82DA2F9E BF8B53ED


V2U
----------------
MacData is
                        4B435F32 5F56424F 42425941 4C494345
        817807C9 E8826EE1 CFB2F373 26D32195 585BD75A 5140460F
        D9BC7139 82B4D7DA 2AF502F3 BE8952F2 C9B5A8D4 160D09E9
        7165BE50 BC42AE4A 5E8D3B4B A83AEB15 EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85


MacKey is
                        139A77DD 97F7C9A3 D14F30B7 C27A0330


Mtag is
                                                ACB99F03 D04B3310
        8C49EFB1 5566DD7C 2D567035 A55F2B71 FA015271 F42E8A68
```

```
KeyData is
                          2F392FED 08FC8839 9FF07B8B D2E34554
        08F20BBC 72322228 50F5C90A 14F52346 23C4D985 6F8C86A6
        AACD2879 C4B5A626 4104CC9E A0DEF14F 11345D1F 0174389C



OnePassDiffieHellmanCDH(P-256)
------------------------------------------------------------
dsV is
                                            8FED7843 1D82558D
        9006C3DE B06AB58D 9DCCC971 06875C67 25D5F166 255BA90A


QsV_x is
                                            1B1631C5 DC76D378
        A914C967 29D0A594 D54B4F58 845B1D4A 4B6BE739 CA4A18EA


QsV_y is
                                            4F85E4C9 26EE5323
        90AA7CD4 14943537 25E6E804 714AA69D 67072F65 DB625E07


deU is
                                            81426414 5F2F56F2
        E96A8E33 7A128499 3FAF432A 5ABCE59E 867B7291 D507A3AF


QeU_x is
                                            2AF502F3 BE8952F2
        C9B5A8D4 160D09E9 7165BE50 BC42AE4A 5E8D3B4B A83AEB15


QeU_y is
                                            EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85



------------------------------------------------------------
no Key Confirmation
Z is
                                            F9C34B92 ACEA12A0
```

```
        C50760E5 9D06C01F 72A0A5CD 8B1BFDD7 3DC8109A 8F8151B3


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         C5BAF92F 8EBBE330 4A6CF682 764BDC7F
        55947A16 DCDB572A 0A0D20A0 5A47BBC4 37FC7C97 C2700009
        C8837D75 754E5796 CDFF537F 62D87E7F 5D2B6DF6 837367A8


KeyData is
                         C5BAF92F 8EBBE330 4A6CF682 764BDC7F
        55947A16 DCDB572A 0A0D20A0 5A47BBC4 37FC7C97 C2700009
        C8837D75 754E5796 CDFF537F 62D87E7F 5D2B6DF6 837367A8




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
                                            F9C34B92 ACEA12A0
        C50760E5 9D06C01F 72A0A5CD 8B1BFDD7 3DC8109A 8F8151B3


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                            C5BAF92F 8EBBE330
        4A6CF682 764BDC7F 55947A16 DCDB572A 0A0D20A0 5A47BBC4
        37FC7C97 C2700009 C8837D75 754E5796 CDFF537F 62D87E7F
        5D2B6DF6 837367A8 ECE5365E 3F286630 B1D592D7 3906AD5C


MacData is
                                            4B435F31 5F56424F
        42425941 4C494345 2AF502F3 BE8952F2 C9B5A8D4 160D09E9
        7165BE50 BC42AE4A 5E8D3B4B A83AEB15 EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85
```

MacKey is
                        C5BAF92F 8EBBE330 4A6CF682 764BDC7F

Mtag is
                                          0913AAAB 61FBE46A
        F3BDCA05 8690A909 214144EC 8370C5EA C376EA45 38EE01FD

KeyData is
                        55947A16 DCDB572A 0A0D20A0 5A47BBC4
        37FC7C97 C2700009 C8837D75 754E5796 CDFF537F 62D87E7F
        5D2B6DF6 837367A8 ECE5365E 3F286630 B1D592D7 3906AD5C

StaticUnifiedCDH(P-256)
----
dsU is
                                          5DCDF2A3 3538D7CF
        93A3680D 4CB4E86A 6814DA67 AC5D8323 EDBAAA59 FAAA2DE4

QsU_x is
                                          E960C4EA 199B35D5
        4CA122BB D85A61A3 0015FB9C 1FA43BE5 C04B4642 7D5206AB

QsU_y is
                                          4EF04F38 77329ACF
        60A13454 CC169266 6497DD57 B8705B0F C9459649 7E433532

dsV is
                                          8FED7843 1D82558D
        9006C3DE B06AB58D 9DCCC971 06875C67 25D5F166 255BA90A

QsV_x is
                                          1B1631C5 DC76D378
        A914C967 29D0A594 D54B4F58 845B1D4A 4B6BE739 CA4A18EA

QsV_y is
                                          4F85E4C9 26EE5323

```
        90AA7CD4 14943537 25E6E804 714AA69D 67072F65 DB625E07



------------------------------------------------------------
no Key Confirmation
NonceU is
                                                817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


Z is
                                                227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


OtherInfo is
                                         1234 56789ABC DEF0414C
        49434531 32330001 817807C9 E8826EE1 CFB2F373 26D32195
        585BD75A 5140460F D9BC7139 82B4D7DA 424F4242 59343536


DerivedKeyMaterial is
                            D34157A9 2C809C89 3E78FED7 AFDEA43C
        FCC7F7E5 58CA9000 6E088BB4 74807F24 0843FE79 01A7CCF6
        911177D2 A3E3FB36 321D9789 D01E656E CA32C417 968118A9


KeyData is
                            D34157A9 2C809C89 3E78FED7 AFDEA43C
        FCC7F7E5 58CA9000 6E088BB4 74807F24 0843FE79 01A7CCF6
        911177D2 A3E3FB36 321D9789 D01E656E CA32C417 968118A9



------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceU is
                                                817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


NonceV is
                                                604063F3 8D0FCEFB
```

```
        132880D3 29415F5A 701EFD62 6E35E72B F38A29DF 2FD653C3


Z is
                                            227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


OtherInfo is
                                       1234 56789ABC DEF0414C
        49434531 32330001 817807C9 E8826EE1 CFB2F373 26D32195
        585BD75A 5140460F D9BC7139 82B4D7DA 424F4242 59343536


DerivedKeyMaterial is
                                            D34157A9 2C809C89
        3E78FED7 AFDEA43C FCC7F7E5 58CA9000 6E088BB4 74807F24
        0843FE79 01A7CCF6 911177D2 A3E3FB36 321D9789 D01E656E
        CA32C417 968118A9 23B4925A 0989E5B5 60A38121 36A0B617


MacData is
                                            4B435F31 5F55414C
        49434542 4F424259 817807C9 E8826EE1 CFB2F373 26D32195
        585BD75A 5140460F D9BC7139 82B4D7DA 604063F3 8D0FCEFB
        132880D3 29415F5A 701EFD62 6E35E72B F38A29DF 2FD653C3


MacKey is
                         D34157A9 2C809C89 3E78FED7 AFDEA43C


Mtag is
                                            11358781 D1E2865F
        8206A688 ACFBCE80 F8D78325 2D6C0DB9 988D656D 92EB083B


KeyData is
                         FCC7F7E5 58CA9000 6E088BB4 74807F24
        0843FE79 01A7CCF6 911177D2 A3E3FB36 321D9789 D01E656E
        CA32C417 968118A9 23B4925A 0989E5B5 60A38121 36A0B617



-------------------------------------------------------------
```

Scheme Responder, Key Confirmation Provider: V to U
NonceV is
                                                604063F3 8D0FCEFB
        132880D3 29415F5A 701EFD62 6E35E72B F38A29DF 2FD653C3

NonceU is
                                                817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA

Z is
                                                227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F

OtherInfo is
                                        1234 56789ABC DEF0414C
        49434531 32330001 817807C9 E8826EE1 CFB2F373 26D32195
        585BD75A 5140460F D9BC7139 82B4D7DA 424F4242 59343536

DerivedKeyMaterial is
                                                D34157A9 2C809C89
        3E78FED7 AFDEA43C FCC7F7E5 58CA9000 6E088BB4 74807F24
        0843FE79 01A7CCF6 911177D2 A3E3FB36 321D9789 D01E656E
        CA32C417 968118A9 23B4925A 0989E5B5 60A38121 36A0B617

MacData is
        4B435F31 5F56424F 42425941 4C494345 817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA

MacKey is
                        D34157A9 2C809C89 3E78FED7 AFDEA43C

Mtag is
                                                7EE04628 20045443
        52E6A270 37B64D7F 39DAC02F A69A462E 14E89AF8 74BAEBC2

KeyData is
                        FCC7F7E5 58CA9000 6E088BB4 74807F24
        0843FE79 01A7CCF6 911177D2 A3E3FB36 321D9789 D01E656E

```
        CA32C417 968118A9 23B4925A 0989E5B5 60A38121 36A0B617



-------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
NonceU is
                                                817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


NonceV is
                                                604063F3 8D0FCEFB
        132880D3 29415F5A 701EFD62 6E35E72B F38A29DF 2FD653C3


Z is
                                                227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


OtherInfo is
                                          1234 56789ABC DEF0414C
        49434531 32330001 817807C9 E8826EE1 CFB2F373 26D32195
        585BD75A 5140460F D9BC7139 82B4D7DA 424F4242 59343536


DerivedKeyMaterial is
                                                D34157A9 2C809C89
        3E78FED7 AFDEA43C FCC7F7E5 58CA9000 6E088BB4 74807F24
        0843FE79 01A7CCF6 911177D2 A3E3FB36 321D9789 D01E656E
        CA32C417 968118A9 23B4925A 0989E5B5 60A38121 36A0B617


U2V
----------------
MacData is
                                                4B435F32 5F55414C
        49434542 4F424259 817807C9 E8826EE1 CFB2F373 26D32195
        585BD75A 5140460F D9BC7139 82B4D7DA 604063F3 8D0FCEFB
        132880D3 29415F5A 701EFD62 6E35E72B F38A29DF 2FD653C3


MacKey is
```

```
                        D34157A9 2C809C89 3E78FED7 AFDEA43C


Mtag is
                                                 BC463927 0152563D
        FE332A90 77F13CD0 7D11D268 BFA9D1E4 C357E016 2E442A13


V2U
----------------
MacData is
                                                 4B435F32 5F56424F
        42425941 4C494345 604063F3 8D0FCEFB 132880D3 29415F5A
        701EFD62 6E35E72B F38A29DF 2FD653C3 817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


MacKey is
                        D34157A9 2C809C89 3E78FED7 AFDEA43C


Mtag is
                                                 955BA1CD 519C6218
        4A1A8EDA DA578889 F1F2304D 91542FCF 3B163EE6 11FA0221


KeyData is
                        FCC7F7E5 58CA9000 6E088BB4 74807F24
        0843FE79 01A7CCF6 911177D2 A3E3FB36 321D9789 D01E656E
        CA32C417 968118A9 23B4925A 0989E5B5 60A38121 36A0B617
```

FullUnifiedCDH(P-384)
---
dsU is
AA46C475 14D92CB6 F565A3AE 500944F6 760D9E74 F646D3D8
9FD09E76 85C41C1F 8DCEC4D7 FA5F91E2 23624A0B EF2FEF93

QsU_x is
B6E49C4B 30E3E642 843D84F4 8ED7D5FE 7254A0BD 057137EE
77F1F9EE D74DB4C8 C43B2010 65B8009E 9A925F3D 7040BDFF

QsU_y is
F502B3F9 841EA18B D8045102 CA2ED057 19CBC63F A338252D
EB0A1154 7B948938 265509B3 E2F4C848 4C7FA78F 321A1A15

dsV is
E7B8C2B3 E5422ACF C314D93D AD7B0025 730A0B38 0F13E4FE
03BDC0E0 0D9D63DA DF4AD600 EBFAA552 57B6DADC B772BB3A

QsV_x is
42B512E1 5235D548 457B651D 9AC448E7 8872DB45 854C4D48
F0F8FCDF 31579B43 0977406B 2008B94E D061D61B BF6B1BBB

QsV_y is
BFB3ED9E 7A69D765 EFDA14DE 7D0D8ECF 9B8BB3A0 3821EE88
8F5B45E9 DF755F55 292F9263 C765C463 B3FE786E 0C909A9D

deU is
D27335EA 71664AF2 44DD14E9 FD126071 5DFD8A79 65571C48
D709EE7A 7962A156 D706A90C BCB5DF29 86F05FEA DB9376F1

QeU_x is
793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66

QeU_y is
C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0

```
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128


deV is
        52D1791F DB4B70F8 9C0F00D4 56C2F702 3B612526 2C36A7DF
        1F802311 21CCE3D3 9BE52E00 C194A413 2C4A6C76 8BCD94D2


QeV_x is
        5CD42AB9 C41B5347 F74B8D4E FB708B3D 5B36DB65 915359B4
        4ABC1764 7B6B9999 789D72A8 4865AE2F 223F12B5 A1ABC120


QeV_y is
        E171458F EAA939AA A3A8BFAC 46B404BD 8F6D5B34 8C0FA4D8
        0CECA163 56CA9332 40BDE872 3415A8EC E035B0ED F36755DE




------------------------------------------------------------
no Key Confirmation
Zs is
        88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
        7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030


Ze is
        5EA1FC4A F7256D20 55981B11 0575E0A8 CAE53160 137D904C
        59D926EB 1B8456E4 27AA8A45 40884C37 DE159A58 028ABC0E


Z is
        5EA1FC4A F7256D20 55981B11 0575E0A8 CAE53160 137D904C
        59D926EB 1B8456E4 27AA8A45 40884C37 DE159A58 028ABC0E
        88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
        7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        8E6E265F 2082F14D 34DA23E1 032C9024 834AF015 72B66477
        82411BDD CB84A5DA EE117BA6 FBA6D0EB 2808EF8A B07005EE
```

```
        ABE52D2E FD31121C 7BF9D5FA FC40E00C 6D6DBF39 EF43FE97
        15C7202C DC2DB7E8 2B88D748 EB84258B F84D8582 F2BFD940


KeyData is
        8E6E265F 2082F14D 34DA23E1 032C9024 834AF015 72B66477
        82411BDD CB84A5DA EE117BA6 FBA6D0EB 2808EF8A B07005EE
        ABE52D2E FD31121C 7BF9D5FA FC40E00C 6D6DBF39 EF43FE97
        15C7202C DC2DB7E8 2B88D748 EB84258B F84D8582 F2BFD940




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Zs is
        88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
        7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030


Ze is
        5EA1FC4A F7256D20 55981B11 0575E0A8 CAE53160 137D904C
        59D926EB 1B8456E4 27AA8A45 40884C37 DE159A58 028ABC0E


Z is
        5EA1FC4A F7256D20 55981B11 0575E0A8 CAE53160 137D904C
        59D926EB 1B8456E4 27AA8A45 40884C37 DE159A58 028ABC0E
        88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
        7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        8E6E265F 2082F14D 34DA23E1 032C9024 834AF015 72B66477
        82411BDD CB84A5DA EE117BA6 FBA6D0EB 2808EF8A B07005EE
        ABE52D2E FD31121C 7BF9D5FA FC40E00C 6D6DBF39 EF43FE97
        15C7202C DC2DB7E8 2B88D748 EB84258B F84D8582 F2BFD940
        8FF3FB6C AF48423D 583E7F9B AC45DE1A F19F3610 8ADB13F7


MacData is
                        4B435F31 5F55414C 49434542 4F424259
```

793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128
5CD42AB9 C41B5347 F74B8D4E FB708B3D 5B36DB65 915359B4
4ABC1764 7B6B9999 789D72A8 4865AE2F 223F12B5 A1ABC120
E171458F EAA939AA A3A8BFAC 46B404BD 8F6D5B34 8C0FA4D8
0CECA163 56CA9332 40BDE872 3415A8EC E035B0ED F36755DE

MacKey is
8E6E265F 2082F14D 34DA23E1 032C9024 834AF015 72B66477

Mtag is
48D78F1B A30800FD 7FA839ED 950A5FDD F885A572 A4EE2F41
C75B577B 39FEDC4E C8412235 A4F05EC0 B614B2EB D15FE6EE

KeyData is
82411BDD CB84A5DA EE117BA6 FBA6D0EB 2808EF8A B07005EE
ABE52D2E FD31121C 7BF9D5FA FC40E00C 6D6DBF39 EF43FE97
15C7202C DC2DB7E8 2B88D748 EB84258B F84D8582 F2BFD940
8FF3FB6C AF48423D 583E7F9B AC45DE1A F19F3610 8ADB13F7

Scheme Responder, Key Confirmation Provider: V to U
Zs is
88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030

Ze is
5EA1FC4A F7256D20 55981B11 0575E0A8 CAE53160 137D904C
59D926EB 1B8456E4 27AA8A45 40884C37 DE159A58 028ABC0E

Z is
5EA1FC4A F7256D20 55981B11 0575E0A8 CAE53160 137D904C
59D926EB 1B8456E4 27AA8A45 40884C37 DE159A58 028ABC0E
88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        8E6E265F 2082F14D 34DA23E1 032C9024 834AF015 72B66477
        82411BDD CB84A5DA EE117BA6 FBA6D0EB 2808EF8A B07005EE
        ABE52D2E FD31121C 7BF9D5FA FC40E00C 6D6DBF39 EF43FE97
        15C7202C DC2DB7E8 2B88D748 EB84258B F84D8582 F2BFD940
        8FF3FB6C AF48423D 583E7F9B AC45DE1A F19F3610 8ADB13F7


MacData is
                        4B435F31 5F56424F 42425941 4C494345
        5CD42AB9 C41B5347 F74B8D4E FB708B3D 5B36DB65 915359B4
        4ABC1764 7B6B9999 789D72A8 4865AE2F 223F12B5 A1ABC120
        E171458F EAA939AA A3A8BFAC 46B404BD 8F6D5B34 8C0FA4D8
        0CECA163 56CA9332 40BDE872 3415A8EC E035B0ED F36755DE
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128


MacKey is
        8E6E265F 2082F14D 34DA23E1 032C9024 834AF015 72B66477


Mtag is
        2A4E289B B91D49E2 C11FA97A 52BB78B2 CCAAC949 FD218381
        442B3840 168F33F3 09728F38 BC93972B F1C121ED D0F5D01E


KeyData is
        82411BDD CB84A5DA EE117BA6 FBA6D0EB 2808EF8A B07005EE
        ABE52D2E FD31121C 7BF9D5FA FC40E00C 6D6DBF39 EF43FE97
        15C7202C DC2DB7E8 2B88D748 EB84258B F84D8582 F2BFD940
        8FF3FB6C AF48423D 583E7F9B AC45DE1A F19F3610 8ADB13F7




-------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
Zs is
```

```
        88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
        7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030


Ze is
        5EA1FC4A F7256D20 55981B11 0575E0A8 CAE53160 137D904C
        59D926EB 1B8456E4 27AA8A45 40884C37 DE159A58 028ABC0E


Z is
        5EA1FC4A F7256D20 55981B11 0575E0A8 CAE53160 137D904C
        59D926EB 1B8456E4 27AA8A45 40884C37 DE159A58 028ABC0E
        88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
        7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        8E6E265F 2082F14D 34DA23E1 032C9024 834AF015 72B66477
        82411BDD CB84A5DA EE117BA6 FBA6D0EB 2808EF8A B07005EE
        ABE52D2E FD31121C 7BF9D5FA FC40E00C 6D6DBF39 EF43FE97
        15C7202C DC2DB7E8 2B88D748 EB84258B F84D8582 F2BFD940
        8FF3FB6C AF48423D 583E7F9B AC45DE1A F19F3610 8ADB13F7


U2V
----------------
MacData is
                        4B435F32 5F55414C 49434542 4F424259
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128
        5CD42AB9 C41B5347 F74B8D4E FB708B3D 5B36DB65 915359B4
        4ABC1764 7B6B9999 789D72A8 4865AE2F 223F12B5 A1ABC120
        E171458F EAA939AA A3A8BFAC 46B404BD 8F6D5B34 8C0FA4D8
        0CECA163 56CA9332 40BDE872 3415A8EC E035B0ED F36755DE


MacKey is
        8E6E265F 2082F14D 34DA23E1 032C9024 834AF015 72B66477
```

```
Mtag is
        4B86C08B FEF2B461 8FDA5905 4CE94123 35C8E24F 089356FC
        4CC07E78 832577D3 2565588B 16D48691 2A18185A 81CDEDB1


V2U
----------------
MacData is
                         4B435F32 5F56424F 42425941 4C494345
        5CD42AB9 C41B5347 F74B8D4E FB708B3D 5B36DB65 915359B4
        4ABC1764 7B6B9999 789D72A8 4865AE2F 223F12B5 A1ABC120
        E171458F EAA939AA A3A8BFAC 46B404BD 8F6D5B34 8C0FA4D8
        0CECA163 56CA9332 40BDE872 3415A8EC E035B0ED F36755DE
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128


MacKey is
        8E6E265F 2082F14D 34DA23E1 032C9024 834AF015 72B66477


Mtag is
        AD9D7DD1 A85FD7F8 F2F3128C 732C84F5 6853A630 4FC60D57
        E1A11B24 F6A55E72 B43EE727 DDBB159F 9CD76A4E 175A75BA


KeyData is
        82411BDD CB84A5DA EE117BA6 FBA6D0EB 2808EF8A B07005EE
        ABE52D2E FD31121C 7BF9D5FA FC40E00C 6D6DBF39 EF43FE97
        15C7202C DC2DB7E8 2B88D748 EB84258B F84D8582 F2BFD940
        8FF3FB6C AF48423D 583E7F9B AC45DE1A F19F3610 8ADB13F7




FullMQV(P-384)
------------------------------------------------------------
dsU is
        AA46C475 14D92CB6 F565A3AE 500944F6 760D9E74 F646D3D8
        9FD09E76 85C41C1F 8DCEC4D7 FA5F91E2 23624A0B EF2FEF93


QsU_x is
        B6E49C4B 30E3E642 843D84F4 8ED7D5FE 7254A0BD 057137EE
```

77F1F9EE D74DB4C8 C43B2010 65B8009E 9A925F3D 7040BDFF

QsU_y is
F502B3F9 841EA18B D8045102 CA2ED057 19CBC63F A338252D
EB0A1154 7B948938 265509B3 E2F4C848 4C7FA78F 321A1A15

dsV is
E7B8C2B3 E5422ACF C314D93D AD7B0025 730A0B38 0F13E4FE
03BDC0E0 0D9D63DA DF4AD600 EBFAA552 57B6DADC B772BB3A

QsV_x is
42B512E1 5235D548 457B651D 9AC448E7 8872DB45 854C4D48
F0F8FCDF 31579B43 0977406B 2008B94E D061D61B BF6B1BBB

QsV_y is
BFB3ED9E 7A69D765 EFDA14DE 7D0D8ECF 9B8BB3A0 3821EE88
8F5B45E9 DF755F55 292F9263 C765C463 B3FE786E 0C909A9D

deU is
D27335EA 71664AF2 44DD14E9 FD126071 5DFD8A79 65571C48
D709EE7A 7962A156 D706A90C BCB5DF29 86F05FEA DB9376F1

QeU_x is
793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66

QeU_y is
C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128

deV is
52D1791F DB4B70F8 9C0F00D4 56C2F702 3B612526 2C36A7DF
1F802311 21CCE3D3 9BE52E00 C194A413 2C4A6C76 8BCD94D2

QeV_x is
5CD42AB9 C41B5347 F74B8D4E FB708B3D 5B36DB65 915359B4
4ABC1764 7B6B9999 789D72A8 4865AE2F 223F12B5 A1ABC120

```
QeV_y is
        E171458F EAA939AA A3A8BFAC 46B404BD 8F6D5B34 8C0FA4D8
        0CECA163 56CA9332 40BDE872 3415A8EC E035B0ED F36755DE




------------------------------------------------------------
no Key Confirmation
Z is
        25329E26 86FFA271 D821F39C 1D3CD1FA F0D5CA3E 0BF60F30
        57D62674 036DE771 50EDCE94 B28E5D21 1F8DFF9C 4C1199AB


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        1DF6B2E9 313FEE5A B5F7B447 57AB1F9C 061EB276 96F3C0F3
        F42D63B8 752801BE 1CCE0D03 AB484B7A 26F2DAD0 47FD20B5
        D2B79935 518D47C1 B1FD69B7 B118DE21 CB8ABC6C B0C07020
        AAD2CBB3 B24B6497 CFCBE174 07D619EA EBD49141 BCB3A42C


KeyData is
        1DF6B2E9 313FEE5A B5F7B447 57AB1F9C 061EB276 96F3C0F3
        F42D63B8 752801BE 1CCE0D03 AB484B7A 26F2DAD0 47FD20B5
        D2B79935 518D47C1 B1FD69B7 B118DE21 CB8ABC6C B0C07020
        AAD2CBB3 B24B6497 CFCBE174 07D619EA EBD49141 BCB3A42C




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Z is
        25329E26 86FFA271 D821F39C 1D3CD1FA F0D5CA3E 0BF60F30
        57D62674 036DE771 50EDCE94 B28E5D21 1F8DFF9C 4C1199AB


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536
```

```
DerivedKeyMaterial is
        1DF6B2E9 313FEE5A B5F7B447 57AB1F9C 061EB276 96F3C0F3
        F42D63B8 752801BE 1CCE0D03 AB484B7A 26F2DAD0 47FD20B5
        D2B79935 518D47C1 B1FD69B7 B118DE21 CB8ABC6C B0C07020
        AAD2CBB3 B24B6497 CFCBE174 07D619EA EBD49141 BCB3A42C
        9103992A 26E24A91 09E4AE20 5272C3D4 1F479F8B 1BF6E931


MacData is
                         4B435F31 5F55414C 49434542 4F424259
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128
        5CD42AB9 C41B5347 F74B8D4E FB708B3D 5B36DB65 915359B4
        4ABC1764 7B6B9999 789D72A8 4865AE2F 223F12B5 A1ABC120
        E171458F EAA939AA A3A8BFAC 46B404BD 8F6D5B34 8C0FA4D8
        0CECA163 56CA9332 40BDE872 3415A8EC E035B0ED F36755DE


MacKey is
        1DF6B2E9 313FEE5A B5F7B447 57AB1F9C 061EB276 96F3C0F3


Mtag is
        A139D711 09C0EFC1 6609A7A1 9425156F 726FA351 E80DEC4D
        2BC15183 ECCE8B41 1004983D 9CF996DA FFF152E7 1BD70B0A


KeyData is
        F42D63B8 752801BE 1CCE0D03 AB484B7A 26F2DAD0 47FD20B5
        D2B79935 518D47C1 B1FD69B7 B118DE21 CB8ABC6C B0C07020
        AAD2CBB3 B24B6497 CFCBE174 07D619EA EBD49141 BCB3A42C
        9103992A 26E24A91 09E4AE20 5272C3D4 1F479F8B 1BF6E931




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
        25329E26 86FFA271 D821F39C 1D3CD1FA F0D5CA3E 0BF60F30
        57D62674 036DE771 50EDCE94 B28E5D21 1F8DFF9C 4C1199AB
```

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
        1DF6B2E9 313FEE5A B5F7B447 57AB1F9C 061EB276 96F3C0F3
        F42D63B8 752801BE 1CCE0D03 AB484B7A 26F2DAD0 47FD20B5
        D2B79935 518D47C1 B1FD69B7 B118DE21 CB8ABC6C B0C07020
        AAD2CBB3 B24B6497 CFCBE174 07D619EA EBD49141 BCB3A42C
        9103992A 26E24A91 09E4AE20 5272C3D4 1F479F8B 1BF6E931

MacData is
                        4B435F31 5F56424F 42425941 4C494345
        5CD42AB9 C41B5347 F74B8D4E FB708B3D 5B36DB65 915359B4
        4ABC1764 7B6B9999 789D72A8 4865AE2F 223F12B5 A1ABC120
        E171458F EAA939AA A3A8BFAC 46B404BD 8F6D5B34 8C0FA4D8
        0CECA163 56CA9332 40BDE872 3415A8EC E035B0ED F36755DE
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128

MacKey is
        1DF6B2E9 313FEE5A B5F7B447 57AB1F9C 061EB276 96F3C0F3

Mtag is
        1DF9E920 5DB9591F DECB0DC6 892B1AD9 CFC9C38A 27D7F345
        9CB2CBDC 95B92672 480DCB77 2861656B A9C9E5BD 7D5A1467

KeyData is
        F42D63B8 752801BE 1CCE0D03 AB484B7A 26F2DAD0 47FD20B5
        D2B79935 518D47C1 B1FD69B7 B118DE21 CB8ABC6C B0C07020
        AAD2CBB3 B24B6497 CFCBE174 07D619EA EBD49141 BCB3A42C
        9103992A 26E24A91 09E4AE20 5272C3D4 1F479F8B 1BF6E931

Scheme Initiator, Key Confirmation Bilateral
Z is

```
        25329E26 86FFA271 D821F39C 1D3CD1FA F0D5CA3E 0BF60F30
        57D62674 036DE771 50EDCE94 B28E5D21 1F8DFF9C 4C1199AB


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        1DF6B2E9 313FEE5A B5F7B447 57AB1F9C 061EB276 96F3C0F3
        F42D63B8 752801BE 1CCE0D03 AB484B7A 26F2DAD0 47FD20B5
        D2B79935 518D47C1 B1FD69B7 B118DE21 CB8ABC6C B0C07020
        AAD2CBB3 B24B6497 CFCBE174 07D619EA EBD49141 BCB3A42C
        9103992A 26E24A91 09E4AE20 5272C3D4 1F479F8B 1BF6E931


U2V
----------------
MacData is
                        4B435F32 5F55414C 49434542 4F424259
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128
        5CD42AB9 C41B5347 F74B8D4E FB708B3D 5B36DB65 915359B4
        4ABC1764 7B6B9999 789D72A8 4865AE2F 223F12B5 A1ABC120
        E171458F EAA939AA A3A8BFAC 46B404BD 8F6D5B34 8C0FA4D8
        0CECA163 56CA9332 40BDE872 3415A8EC E035B0ED F36755DE


MacKey is
        1DF6B2E9 313FEE5A B5F7B447 57AB1F9C 061EB276 96F3C0F3


Mtag is
        096852B0 1E118249 E4B7A1E1 9BE128AC 147EB34B 19B0135B
        D61D33EC FC5CBEC1 EE6079AA 965C1C6A C2FEAEBF BB41E846


V2U
----------------
MacData is
                        4B435F32 5F56424F 42425941 4C494345
        5CD42AB9 C41B5347 F74B8D4E FB708B3D 5B36DB65 915359B4
        4ABC1764 7B6B9999 789D72A8 4865AE2F 223F12B5 A1ABC120
        E171458F EAA939AA A3A8BFAC 46B404BD 8F6D5B34 8C0FA4D8
```

```
        0CECA163 56CA9332 40BDE872 3415A8EC E035B0ED F36755DE
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128


MacKey is
        1DF6B2E9 313FEE5A B5F7B447 57AB1F9C 061EB276 96F3C0F3


Mtag is
        F91066DE D3765AFA FE5006C6 E6B193EF B3EAB284 8B7042CC
        37EA3302 8D52AE92 3BC9FBF1 F943FE06 CAF93CCD 01740218


KeyData is
        F42D63B8 752801BE 1CCE0D03 AB484B7A 26F2DAD0 47FD20B5
        D2B79935 518D47C1 B1FD69B7 B118DE21 CB8ABC6C B0C07020
        AAD2CBB3 B24B6497 CFCBE174 07D619EA EBD49141 BCB3A42C
        9103992A 26E24A91 09E4AE20 5272C3D4 1F479F8B 1BF6E931




EphemeralUnifiedCDH(P-384)
------------------------------------------------------------
deU is
        D27335EA 71664AF2 44DD14E9 FD126071 5DFD8A79 65571C48
        D709EE7A 7962A156 D706A90C BCB5DF29 86F05FEA DB9376F1


QeU_x is
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66


QeU_y is
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128


deV is
        52D1791F DB4B70F8 9C0F00D4 56C2F702 3B612526 2C36A7DF
        1F802311 21CCE3D3 9BE52E00 C194A413 2C4A6C76 8BCD94D2
```

```
QeV_x is
        5CD42AB9 C41B5347 F74B8D4E FB708B3D 5B36DB65 915359B4
        4ABC1764 7B6B9999 789D72A8 4865AE2F 223F12B5 A1ABC120


QeV_y is
        E171458F EAA939AA A3A8BFAC 46B404BD 8F6D5B34 8C0FA4D8
        0CECA163 56CA9332 40BDE872 3415A8EC E035B0ED F36755DE




------------------------------------------------------------
no Key Confirmation
Z is
        5EA1FC4A F7256D20 55981B11 0575E0A8 CAE53160 137D904C
        59D926EB 1B8456E4 27AA8A45 40884C37 DE159A58 028ABC0E


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        95824CDC 9774A4F2 5A9DD4C2 C18A604E 0F103E54 0E80EBD7
        8DD260C1 520C6E54 3C558DFB 429CCC81 FDD3DDE2 3A5DD1A6
        89813FF1 17E2A33E 52A7DAE0 996F857E 99B2B5C7 4365642A
        FE953EAB 155766B9 C78AE255 A74622CE DD505304 3FA716EE


KeyData is
        95824CDC 9774A4F2 5A9DD4C2 C18A604E 0F103E54 0E80EBD7
        8DD260C1 520C6E54 3C558DFB 429CCC81 FDD3DDE2 3A5DD1A6
        89813FF1 17E2A33E 52A7DAE0 996F857E 99B2B5C7 4365642A
        FE953EAB 155766B9 C78AE255 A74622CE DD505304 3FA716EE




OnePassUnifiedCDH(P-384)
------------------------------------------------------------
dsU is
        AA46C475 14D92CB6 F565A3AE 500944F6 760D9E74 F646D3D8
        9FD09E76 85C41C1F 8DCEC4D7 FA5F91E2 23624A0B EF2FEF93
```

```
QsU_x is
        B6E49C4B 30E3E642 843D84F4 8ED7D5FE 7254A0BD 057137EE
        77F1F9EE D74DB4C8 C43B2010 65B8009E 9A925F3D 7040BDFF


QsU_y is
        F502B3F9 841EA18B D8045102 CA2ED057 19CBC63F A338252D
        EB0A1154 7B948938 265509B3 E2F4C848 4C7FA78F 321A1A15


dsV is
        E7B8C2B3 E5422ACF C314D93D AD7B0025 730A0B38 0F13E4FE
        03BDC0E0 0D9D63DA DF4AD600 EBFAA552 57B6DADC B772BB3A


QsV_x is
        42B512E1 5235D548 457B651D 9AC448E7 8872DB45 854C4D48
        F0F8FCDF 31579B43 0977406B 2008B94E D061D61B BF6B1BBB


QsV_y is
        BFB3ED9E 7A69D765 EFDA14DE 7D0D8ECF 9B8BB3A0 3821EE88
        8F5B45E9 DF755F55 292F9263 C765C463 B3FE786E 0C909A9D


deU is
        D27335EA 71664AF2 44DD14E9 FD126071 5DFD8A79 65571C48
        D709EE7A 7962A156 D706A90C BCB5DF29 86F05FEA DB9376F1


QeU_x is
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66


QeU_y is
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128




------------------------------------------------------------
no Key Confirmation
Zs is
```

88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030

Ze is
B2672A91 6BE1EC91 F6A2C618 74735152 B081949C 1FF53D1E
0BC2BC29 87985A40 7AD10961 0AC0990F 8ED2867E AC2D34DF

Z is
B2672A91 6BE1EC91 F6A2C618 74735152 B081949C 1FF53D1E
0BC2BC29 87985A40 7AD10961 0AC0990F 8ED2867E AC2D34DF
88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
BBB8BB84 83D17952 2D15241A 237D6C08 BD3C0161 CD3349EF
9F685494 DA85750C E7B5B585 621DDF3E 161BA9EB 253E61B4
82117082 1EC98372 C50DA5A1 B5480CCB A738E877 A2FC9081
A1C20484 9A93431A 4B959596 8340D8D1 98E64BA0 68F3856C

KeyData is
BBB8BB84 83D17952 2D15241A 237D6C08 BD3C0161 CD3349EF
9F685494 DA85750C E7B5B585 621DDF3E 161BA9EB 253E61B4
82117082 1EC98372 C50DA5A1 B5480CCB A738E877 A2FC9081
A1C20484 9A93431A 4B959596 8340D8D1 98E64BA0 68F3856C

Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988

Zs is
88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030

Ze is
        B2672A91 6BE1EC91 F6A2C618 74735152 B081949C 1FF53D1E
        0BC2BC29 87985A40 7AD10961 0AC0990F 8ED2867E AC2D34DF

Z is
        B2672A91 6BE1EC91 F6A2C618 74735152 B081949C 1FF53D1E
        0BC2BC29 87985A40 7AD10961 0AC0990F 8ED2867E AC2D34DF
        88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
        7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
        BBB8BB84 83D17952 2D15241A 237D6C08 BD3C0161 CD3349EF
        9F685494 DA85750C E7B5B585 621DDF3E 161BA9EB 253E61B4
        82117082 1EC98372 C50DA5A1 B5480CCB A738E877 A2FC9081
        A1C20484 9A93431A 4B959596 8340D8D1 98E64BA0 68F3856C
        2DD07262 81DAC0DD 7818DADC A7A4A8E4 4C540319 811CA08E

MacData is
                        4B435F31 5F55414C 49434542 4F424259
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988

MacKey is
        BBB8BB84 83D17952 2D15241A 237D6C08 BD3C0161 CD3349EF

Mtag is
        30AFDA64 2BCE5992 D861FDEC 68ACD4A7 EA07B9DD F6B5326A
        82608A4F 2A228E52 7F729393 D5A3C13D 4ACE2201 372FA071

KeyData is

9F685494 DA85750C E7B5B585 621DDF3E 161BA9EB 253E61B4
82117082 1EC98372 C50DA5A1 B5480CCB A738E877 A2FC9081
A1C20484 9A93431A 4B959596 8340D8D1 98E64BA0 68F3856C
2DD07262 81DAC0DD 7818DADC A7A4A8E4 4C540319 811CA08E

Scheme Responder, Key Confirmation Provider: V to U
NonceU is
F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988

Zs is
88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030

Ze is
B2672A91 6BE1EC91 F6A2C618 74735152 B081949C 1FF53D1E
0BC2BC29 87985A40 7AD10961 0AC0990F 8ED2867E AC2D34DF

Z is
B2672A91 6BE1EC91 F6A2C618 74735152 B081949C 1FF53D1E
0BC2BC29 87985A40 7AD10961 0AC0990F 8ED2867E AC2D34DF
88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
BBB8BB84 83D17952 2D15241A 237D6C08 BD3C0161 CD3349EF
9F685494 DA85750C E7B5B585 621DDF3E 161BA9EB 253E61B4
82117082 1EC98372 C50DA5A1 B5480CCB A738E877 A2FC9081
A1C20484 9A93431A 4B959596 8340D8D1 98E64BA0 68F3856C
2DD07262 81DAC0DD 7818DADC A7A4A8E4 4C540319 811CA08E

MacData is
4B435F31 5F56424F 42425941 4C494345

793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128

MacKey is
BBB8BB84 83D17952 2D15241A 237D6C08 BD3C0161 CD3349EF

Mtag is
C8A6E9F3 F376380B 42DE44B5 270536AA 81969EE9 DCDBEB05
81C0E644 A7F31274 4B0E47C8 44C11B4A E7F05350 C9A46E93

KeyData is
9F685494 DA85750C E7B5B585 621DDF3E 161BA9EB 253E61B4
82117082 1EC98372 C50DA5A1 B5480CCB A738E877 A2FC9081
A1C20484 9A93431A 4B959596 8340D8D1 98E64BA0 68F3856C
2DD07262 81DAC0DD 7818DADC A7A4A8E4 4C540319 811CA08E

Scheme Initiator, Key Confirmation Bilateral
NonceV is
F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988

Zs is
88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030

Ze is
B2672A91 6BE1EC91 F6A2C618 74735152 B081949C 1FF53D1E
0BC2BC29 87985A40 7AD10961 0AC0990F 8ED2867E AC2D34DF

Z is
B2672A91 6BE1EC91 F6A2C618 74735152 B081949C 1FF53D1E
0BC2BC29 87985A40 7AD10961 0AC0990F 8ED2867E AC2D34DF
88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        BBB8BB84 83D17952 2D15241A 237D6C08 BD3C0161 CD3349EF
        9F685494 DA85750C E7B5B585 621DDF3E 161BA9EB 253E61B4
        82117082 1EC98372 C50DA5A1 B5480CCB A738E877 A2FC9081
        A1C20484 9A93431A 4B959596 8340D8D1 98E64BA0 68F3856C
        2DD07262 81DAC0DD 7818DADC A7A4A8E4 4C540319 811CA08E


U2V
----------------
MacData is
                        4B435F32 5F55414C 49434542 4F424259
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988


MacKey is
        BBB8BB84 83D17952 2D15241A 237D6C08 BD3C0161 CD3349EF


Mtag is
        8BAE5D2C F589947A D2619F1A D07FC5F0 5DF4685F AF36DFD7
        3F70D1C6 10C98890 D97FE138 023CE4B7 47C7FC2F 84610FB6


V2U
----------------
MacData is
                        4B435F32 5F56424F 42425941 4C494345
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128
```

MacKey is
        BBB8BB84 83D17952 2D15241A 237D6C08 BD3C0161 CD3349EF

Mtag is
        FB92A939 E1E6B83F D74FA8D2 29DD7219 E238E900 C917C8E1
        F570E908 007A97E3 E72F1EAC F8259620 67AE57A2 BE873EE7

KeyData is
        9F685494 DA85750C E7B5B585 621DDF3E 161BA9EB 253E61B4
        82117082 1EC98372 C50DA5A1 B5480CCB A738E877 A2FC9081
        A1C20484 9A93431A 4B959596 8340D8D1 98E64BA0 68F3856C
        2DD07262 81DAC0DD 7818DADC A7A4A8E4 4C540319 811CA08E

OnePassMQV(P-384)
---
dsU is
        AA46C475 14D92CB6 F565A3AE 500944F6 760D9E74 F646D3D8
        9FD09E76 85C41C1F 8DCEC4D7 FA5F91E2 23624A0B EF2FEF93

QsU_x is
        B6E49C4B 30E3E642 843D84F4 8ED7D5FE 7254A0BD 057137EE
        77F1F9EE D74DB4C8 C43B2010 65B8009E 9A925F3D 7040BDFF

QsU_y is
        F502B3F9 841EA18B D8045102 CA2ED057 19CBC63F A338252D
        EB0A1154 7B948938 265509B3 E2F4C848 4C7FA78F 321A1A15

dsV is
        E7B8C2B3 E5422ACF C314D93D AD7B0025 730A0B38 0F13E4FE
        03BDC0E0 0D9D63DA DF4AD600 EBFAA552 57B6DADC B772BB3A

QsV_x is
        42B512E1 5235D548 457B651D 9AC448E7 8872DB45 854C4D48
        F0F8FCDF 31579B43 0977406B 2008B94E D061D61B BF6B1BBB

```
QsV_y is
        BFB3ED9E 7A69D765 EFDA14DE 7D0D8ECF 9B8BB3A0 3821EE88
        8F5B45E9 DF755F55 292F9263 C765C463 B3FE786E 0C909A9D


deU is
        D27335EA 71664AF2 44DD14E9 FD126071 5DFD8A79 65571C48
        D709EE7A 7962A156 D706A90C BCB5DF29 86F05FEA DB9376F1


QeU_x is
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66


QeU_y is
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128




------------------------------------------------------------
no Key Confirmation
Z is
        EE9D0DAC 7A2FFA32 F77933D0 91026A94 5D913FDA EB4B8020
        1E19DF45 C1902316 F95BB133 654C8002 D88BF81B EF2F4F6A


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        B95685CB 37D2439F C1EFA320 2A137842 88F4EAD2 D52FBFA0
        0C3017E6 E4979AB7 ECA63546 3374B707 DEB8C25A 6511F5FF
        EB03920C D04F856B 83C78BD9 A35B5EE7 89636982 88C2642C
        2CF15381 CA210529 43551A30 CB5D1847 C4403CEC 5D2807D6


KeyData is
        B95685CB 37D2439F C1EFA320 2A137842 88F4EAD2 D52FBFA0
        0C3017E6 E4979AB7 ECA63546 3374B707 DEB8C25A 6511F5FF
        EB03920C D04F856B 83C78BD9 A35B5EE7 89636982 88C2642C
        2CF15381 CA210529 43551A30 CB5D1847 C4403CEC 5D2807D6
```

```
------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988


Z is
        EE9D0DAC 7A2FFA32 F77933D0 91026A94 5D913FDA EB4B8020
        1E19DF45 C1902316 F95BB133 654C8002 D88BF81B EF2F4F6A


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        B95685CB 37D2439F C1EFA320 2A137842 88F4EAD2 D52FBFA0
        0C3017E6 E4979AB7 ECA63546 3374B707 DEB8C25A 6511F5FF
        EB03920C D04F856B 83C78BD9 A35B5EE7 89636982 88C2642C
        2CF15381 CA210529 43551A30 CB5D1847 C4403CEC 5D2807D6
        D19FABD8 4414764F 513FDD8A 1E45EB79 D8CC4BD2 8792C812


MacData is
                         4B435F31 5F55414C 49434542 4F424259
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988


MacKey is
        B95685CB 37D2439F C1EFA320 2A137842 88F4EAD2 D52FBFA0


Mtag is
        87C99855 88B8D0F9 7F4DC1D8 5E25D6B0 1820DB34 4FBF3468
        FACAE44B 977BFE73 FB9AA595 9539A0C7 CC6DD154 8610F058
```

KeyData is
0C3017E6 E4979AB7 ECA63546 3374B707 DEB8C25A 6511F5FF
EB03920C D04F856B 83C78BD9 A35B5EE7 89636982 88C2642C
2CF15381 CA210529 43551A30 CB5D1847 C4403CEC 5D2807D6
D19FABD8 4414764F 513FDD8A 1E45EB79 D8CC4BD2 8792C812

Scheme Responder, Key Confirmation Provider: V to U
NonceU is
F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988

Z is
EE9D0DAC 7A2FFA32 F77933D0 91026A94 5D913FDA EB4B8020
1E19DF45 C1902316 F95BB133 654C8002 D88BF81B EF2F4F6A

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
B95685CB 37D2439F C1EFA320 2A137842 88F4EAD2 D52FBFA0
0C3017E6 E4979AB7 ECA63546 3374B707 DEB8C25A 6511F5FF
EB03920C D04F856B 83C78BD9 A35B5EE7 89636982 88C2642C
2CF15381 CA210529 43551A30 CB5D1847 C4403CEC 5D2807D6
D19FABD8 4414764F 513FDD8A 1E45EB79 D8CC4BD2 8792C812

MacData is
4B435F31 5F56424F 42425941 4C494345
793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128

MacKey is
B95685CB 37D2439F C1EFA320 2A137842 88F4EAD2 D52FBFA0

Mtag is

```
        D75DECD4 5AFF89A8 D1F1224A 587AA819 2F9F9C85 50145776
        BC55AFC0 C6B6081C 165FD393 61C45F4A BA4B557F 5FF0AC9F


KeyData is
        0C3017E6 E4979AB7 ECA63546 3374B707 DEB8C25A 6511F5FF
        EB03920C D04F856B 83C78BD9 A35B5EE7 89636982 88C2642C
        2CF15381 CA210529 43551A30 CB5D1847 C4403CEC 5D2807D6
        D19FABD8 4414764F 513FDD8A 1E45EB79 D8CC4BD2 8792C812




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988


Z is
        EE9D0DAC 7A2FFA32 F77933D0 91026A94 5D913FDA EB4B8020
        1E19DF45 C1902316 F95BB133 654C8002 D88BF81B EF2F4F6A


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        B95685CB 37D2439F C1EFA320 2A137842 88F4EAD2 D52FBFA0
        0C3017E6 E4979AB7 ECA63546 3374B707 DEB8C25A 6511F5FF
        EB03920C D04F856B 83C78BD9 A35B5EE7 89636982 88C2642C
        2CF15381 CA210529 43551A30 CB5D1847 C4403CEC 5D2807D6
        D19FABD8 4414764F 513FDD8A 1E45EB79 D8CC4BD2 8792C812


U2V
----------------
MacData is
                        4B435F32 5F55414C 49434542 4F424259
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
```

```
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988


MacKey is
        B95685CB 37D2439F C1EFA320 2A137842 88F4EAD2 D52FBFA0


Mtag is
        EEFF3280 6231D206 46383A7F BBF244E2 FF823922 BBDF9EFF
        72FA7908 3E3DBBA1 308A3583 BD65B5FC BAB91282 3E2D7DBF


V2U
----------------
MacData is
                         4B435F32 5F56424F 42425941 4C494345
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128


MacKey is
        B95685CB 37D2439F C1EFA320 2A137842 88F4EAD2 D52FBFA0


Mtag is
        65609F84 0027D9B1 3035EA69 450C4DBE 49A0D34A BFFE2FEA
        EAF67FCC E1093264 A90D2BDF 317FA9C7 D90EE22B 1D916E57


KeyData is
        0C3017E6 E4979AB7 ECA63546 3374B707 DEB8C25A 6511F5FF
        EB03920C D04F856B 83C78BD9 A35B5EE7 89636982 88C2642C
        2CF15381 CA210529 43551A30 CB5D1847 C4403CEC 5D2807D6
        D19FABD8 4414764F 513FDD8A 1E45EB79 D8CC4BD2 8792C812




OnePassDiffieHellmanCDH(P-384)
------------------------------------------------------------
dsV is
        E7B8C2B3 E5422ACF C314D93D AD7B0025 730A0B38 0F13E4FE
```

03BDC0E0 0D9D63DA DF4AD600 EBFAA552 57B6DADC B772BB3A

QsV_x is
42B512E1 5235D548 457B651D 9AC448E7 8872DB45 854C4D48
F0F8FCDF 31579B43 0977406B 2008B94E D061D61B BF6B1BBB

QsV_y is
BFB3ED9E 7A69D765 EFDA14DE 7D0D8ECF 9B8BB3A0 3821EE88
8F5B45E9 DF755F55 292F9263 C765C463 B3FE786E 0C909A9D

deU is
D27335EA 71664AF2 44DD14E9 FD126071 5DFD8A79 65571C48
D709EE7A 7962A156 D706A90C BCB5DF29 86F05FEA DB9376F1

QeU_x is
793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66

QeU_y is
C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128

---

no Key Confirmation
Z is
B2672A91 6BE1EC91 F6A2C618 74735152 B081949C 1FF53D1E
0BC2BC29 87985A40 7AD10961 0AC0990F 8ED2867E AC2D34DF

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
9F14D953 BE79A0F0 19FBEC23 0574FEF2 0FDD37E7 68E01C3E
B5EDDD24 BB2682D9 44731656 7DAA372E FA5CB467 61F50402
A7D7B473 A280DE54 C56D7FE8 56BBD745 52148D85 D7625678
56B080E0 DABE441D 59520D45 14017736 5F9CACF1 1B54DB2E

KeyData is
        9F14D953 BE79A0F0 19FBEC23 0574FEF2 0FDD37E7 68E01C3E
        B5EDDD24 BB2682D9 44731656 7DAA372E FA5CB467 61F50402
        A7D7B473 A280DE54 C56D7FE8 56BBD745 52148D85 D7625678
        56B080E0 DABE441D 59520D45 14017736 5F9CACF1 1B54DB2E

Scheme Responder, Key Confirmation Provider: V to U
Z is
        B2672A91 6BE1EC91 F6A2C618 74735152 B081949C 1FF53D1E
        0BC2BC29 87985A40 7AD10961 0AC0990F 8ED2867E AC2D34DF

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
        9F14D953 BE79A0F0 19FBEC23 0574FEF2 0FDD37E7 68E01C3E
        B5EDDD24 BB2682D9 44731656 7DAA372E FA5CB467 61F50402
        A7D7B473 A280DE54 C56D7FE8 56BBD745 52148D85 D7625678
        56B080E0 DABE441D 59520D45 14017736 5F9CACF1 1B54DB2E
        730EA8FB BFA8FE4A 6227F998 CC4DBA63 6136F159 001059CF

MacData is
                        4B435F31 5F56424F 42425941 4C494345
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128

MacKey is
        9F14D953 BE79A0F0 19FBEC23 0574FEF2 0FDD37E7 68E01C3E

Mtag is
        545245CD CFB724EB 57BA7FD0 B7B21A3D EC7B953E 54A1ABE6
        696D912C 0277EC2E C2830F0B 7E53F58D C2B368A0 5A58093F

KeyData is
	B5EDDD24 BB2682D9 44731656 7DAA372E FA5CB467 61F50402
	A7D7B473 A280DE54 C56D7FE8 56BBD745 52148D85 D7625678
	56B080E0 DABE441D 59520D45 14017736 5F9CACF1 1B54DB2E
	730EA8FB BFA8FE4A 6227F998 CC4DBA63 6136F159 001059CF

StaticUnifiedCDH(P-384)
---
dsU is
	AA46C475 14D92CB6 F565A3AE 500944F6 760D9E74 F646D3D8
	9FD09E76 85C41C1F 8DCEC4D7 FA5F91E2 23624A0B EF2FEF93

QsU_x is
	B6E49C4B 30E3E642 843D84F4 8ED7D5FE 7254A0BD 057137EE
	77F1F9EE D74DB4C8 C43B2010 65B8009E 9A925F3D 7040BDFF

QsU_y is
	F502B3F9 841EA18B D8045102 CA2ED057 19CBC63F A338252D
	EB0A1154 7B948938 265509B3 E2F4C848 4C7FA78F 321A1A15

dsV is
	E7B8C2B3 E5422ACF C314D93D AD7B0025 730A0B38 0F13E4FE
	03BDC0E0 0D9D63DA DF4AD600 EBFAA552 57B6DADC B772BB3A

QsV_x is
	42B512E1 5235D548 457B651D 9AC448E7 8872DB45 854C4D48
	F0F8FCDF 31579B43 0977406B 2008B94E D061D61B BF6B1BBB

QsV_y is
	BFB3ED9E 7A69D765 EFDA14DE 7D0D8ECF 9B8BB3A0 3821EE88
	8F5B45E9 DF755F55 292F9263 C765C463 B3FE786E 0C909A9D

---
no Key Confirmation

```
NonceU is
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988


Z is
        88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
        7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030


OtherInfo is
                                                          1234
        56789ABC DEF0414C 49434531 32338001 F19737D1 F8452AC6
        3510BC35 D3444440 F4DC2C8A EEDBF0F9 ADBA62C9 1DBF5FB7
        DEC1DBDA 032C7F8C E54ACF60 2F922988 424F4242 59343536


DerivedKeyMaterial is
        973A6753 E146E77B 32F134EF 72394029 C0686DC4 3BB6D9EF
        E3291C4A 38399224 CD519938 122C6472 FAF19EE1 4997A2A7
        3A607E72 C639ABD9 A405E086 D1BB79B8 CD9E7C97 B5D8FD56
        DD35593C 8376A0A5 39863BB0 53201319 FCBEFC7C DD5450CB


KeyData is
        973A6753 E146E77B 32F134EF 72394029 C0686DC4 3BB6D9EF
        E3291C4A 38399224 CD519938 122C6472 FAF19EE1 4997A2A7
        3A607E72 C639ABD9 A405E086 D1BB79B8 CD9E7C97 B5D8FD56
        DD35593C 8376A0A5 39863BB0 53201319 FCBEFC7C DD5450CB




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceU is
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988


NonceV is
        5A452352 1700C41A AED50DE4 BA622E46 FADAC9BE 771DBD0F
        95664DF2 D4116AD2 B58136C2 87DE481D A491F4AC 2CAA687F


Z is
```

```
        88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
        7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030


OtherInfo is
                                                          1234
        56789ABC DEF0414C 49434531 32338001 F19737D1 F8452AC6
        3510BC35 D3444440 F4DC2C8A EEDBF0F9 ADBA62C9 1DBF5FB7
        DEC1DBDA 032C7F8C E54ACF60 2F922988 424F4242 59343536


DerivedKeyMaterial is
        973A6753 E146E77B 32F134EF 72394029 C0686DC4 3BB6D9EF
        E3291C4A 38399224 CD519938 122C6472 FAF19EE1 4997A2A7
        3A607E72 C639ABD9 A405E086 D1BB79B8 CD9E7C97 B5D8FD56
        DD35593C 8376A0A5 39863BB0 53201319 FCBEFC7C DD5450CB
        33BDBE3F 58C025CE 51B9196A DB386F8F 5FEB7DF7 AB7433B9


MacData is
                         4B435F31 5F55414C 49434542 4F424259
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988
        5A452352 1700C41A AED50DE4 BA622E46 FADAC9BE 771DBD0F
        95664DF2 D4116AD2 B58136C2 87DE481D A491F4AC 2CAA687F


MacKey is
        973A6753 E146E77B 32F134EF 72394029 C0686DC4 3BB6D9EF


Mtag is
        7638E87E 6D616F2B 3DE4A120 EF20CCAC 21AFD521 69B9E100
        FD426AB7 3AE8A2E7 D9C564F9 E2F9D8C2 27A600DC 1297050C


KeyData is
        E3291C4A 38399224 CD519938 122C6472 FAF19EE1 4997A2A7
        3A607E72 C639ABD9 A405E086 D1BB79B8 CD9E7C97 B5D8FD56
        DD35593C 8376A0A5 39863BB0 53201319 FCBEFC7C DD5450CB
        33BDBE3F 58C025CE 51B9196A DB386F8F 5FEB7DF7 AB7433B9




-------------------------------------------------------------
```

Scheme Responder, Key Confirmation Provider: V to U
NonceV is
        5A452352 1700C41A AED50DE4 BA622E46 FADAC9BE 771DBD0F
        95664DF2 D4116AD2 B58136C2 87DE481D A491F4AC 2CAA687F

NonceU is
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988

Z is
        88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
        7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030

OtherInfo is
                                                        1234
        56789ABC DEF0414C 49434531 32338001 F19737D1 F8452AC6
        3510BC35 D3444440 F4DC2C8A EEDBF0F9 ADBA62C9 1DBF5FB7
        DEC1DBDA 032C7F8C E54ACF60 2F922988 424F4242 59343536

DerivedKeyMaterial is
        973A6753 E146E77B 32F134EF 72394029 C0686DC4 3BB6D9EF
        E3291C4A 38399224 CD519938 122C6472 FAF19EE1 4997A2A7
        3A607E72 C639ABD9 A405E086 D1BB79B8 CD9E7C97 B5D8FD56
        DD35593C 8376A0A5 39863BB0 53201319 FCBEFC7C DD5450CB
        33BDBE3F 58C025CE 51B9196A DB386F8F 5FEB7DF7 AB7433B9

MacData is
                            4B435F31 5F56424F 42425941 4C494345
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988

MacKey is
        973A6753 E146E77B 32F134EF 72394029 C0686DC4 3BB6D9EF

Mtag is
        E39200D9 02F1193F F39B7FB3 683F1BB0 D8945BD2 9D1F6E38
        4B71684A 7B1B92B6 005EB0BA 76FE53B4 3E604498 9820C623

```
KeyData is
        E3291C4A 38399224 CD519938 122C6472 FAF19EE1 4997A2A7
        3A607E72 C639ABD9 A405E086 D1BB79B8 CD9E7C97 B5D8FD56
        DD35593C 8376A0A5 39863BB0 53201319 FCBEFC7C DD5450CB
        33BDBE3F 58C025CE 51B9196A DB386F8F 5FEB7DF7 AB7433B9



------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
NonceU is
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988


NonceV is
        5A452352 1700C41A AED50DE4 BA622E46 FADAC9BE 771DBD0F
        95664DF2 D4116AD2 B58136C2 87DE481D A491F4AC 2CAA687F


Z is
        88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
        7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030


OtherInfo is
                                                          1234
        56789ABC DEF0414C 49434531 32338001 F19737D1 F8452AC6
        3510BC35 D3444440 F4DC2C8A EEDBF0F9 ADBA62C9 1DBF5FB7
        DEC1DBDA 032C7F8C E54ACF60 2F922988 424F4242 59343536


DerivedKeyMaterial is
        973A6753 E146E77B 32F134EF 72394029 C0686DC4 3BB6D9EF
        E3291C4A 38399224 CD519938 122C6472 FAF19EE1 4997A2A7
        3A607E72 C639ABD9 A405E086 D1BB79B8 CD9E7C97 B5D8FD56
        DD35593C 8376A0A5 39863BB0 53201319 FCBEFC7C DD5450CB
        33BDBE3F 58C025CE 51B9196A DB386F8F 5FEB7DF7 AB7433B9


U2V
----------------
MacData is
                          4B435F32 5F55414C 49434542 4F424259
```

```
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988
        5A452352 1700C41A AED50DE4 BA622E46 FADAC9BE 771DBD0F
        95664DF2 D4116AD2 B58136C2 87DE481D A491F4AC 2CAA687F


MacKey is
        973A6753 E146E77B 32F134EF 72394029 C0686DC4 3BB6D9EF


Mtag is
        EB224525 C906CBF9 FF252E37 AF00020E 93D397B5 014A6051
        4062C08F 3949DBD7 D097F22D 691CCC87 7DB2FE64 746F9CEA


V2U
----------------
MacData is
                         4B435F32 5F56424F 42425941 4C494345
        5A452352 1700C41A AED50DE4 BA622E46 FADAC9BE 771DBD0F
        95664DF2 D4116AD2 B58136C2 87DE481D A491F4AC 2CAA687F
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988


MacKey is
        973A6753 E146E77B 32F134EF 72394029 C0686DC4 3BB6D9EF


Mtag is
        1DD2EC31 FFBF133F 9F1908E1 E3F2F206 05EC5675 5D168381
        499D7296 7AD75398 C5DAE6D0 B6DE4EB1 819D199D D77F51A0


KeyData is
        E3291C4A 38399224 CD519938 122C6472 FAF19EE1 4997A2A7
        3A607E72 C639ABD9 A405E086 D1BB79B8 CD9E7C97 B5D8FD56
        DD35593C 8376A0A5 39863BB0 53201319 FCBEFC7C DD5450CB
        33BDBE3F 58C025CE 51B9196A DB386F8F 5FEB7DF7 AB7433B9
```

FullUnifiedCDH(P-521)
----
dsU is
                    017D 1527DCC7 C046E4D3 04600ED0 D3A625F6
        AA46C475 14D92CB6 A6416C1B 8978B3E6 E9796830 6FFC49D0
        0371CCBD 4B796AA3 6547A6ED 3E78BBDF F2CFF34C E4C57FC9

QsU_x is
                    00D0 C2D9A667 F85A3C27 0C838535 04616791
        F3052858 3CF2D5CD D35D4E77 D440FE51 01DFC0E1 953983A9
        C1D7C330 7E6213FB CEB3D113 460D7B45 BBACAE5D 54B68166

QsU_y is
                    01C8 A85F0367 B3B1F4DE 8A74021E 08E13EA5
        65EF012E 647DD317 3B21DD6B B9987155 73063EBB 3152CAA7
        91ABD47F D31FB528 799413F8 DFF76E28 64E9870A 262ECACB

dsV is
                    00A0 752E306C ECD87AB0 E4830DA1 44F8038C
        E7B8C2B3 E5422ACF 9AAA6CCF 21818316 9A4CCA2A D577A64E
        6D86DCBF F5C1727A 11FD1CB8 E3A53842 B84005FD A9AC7F36

QsV_x is
                    0128 C16B23A4 259C9FE4 257C1DA4 3C7735C4
        3337929E 0FD86CC2 A778975B 67184CC2 825F6E66 7876D404
        BBF03E04 1F8FAD2F CCC036CD 5448B64E 9BD7DF6F 537659BB

QsV_y is
                    0108 089A6431 FED52344 DD5859A0 E5432D16
        9BEE36F5 3F857AED 08A69FE3 07B1C94B 8ABDCF65 0C4D1297
        29D69FB7 7D1CC1CD 651C676B 309CE018 C9771EAB 9CA5A754

deU is
                    0113 F82DA825 735E3D97 276683B2 B74277BA
        D27335EA 71664AF2 430CC4F3 3459B966 9EE78B3F FB9B8683
        015D344D CBFEF6FB 9AF4C6C4 70BE2545 16CD3C1A 1FB47362

QeU_x is
01EB B34DD757 21ABF8AD C9DBED17 889CBB97
65D90A7C 60F2CEF0 07BB0F2B 26E14881 FD4442E6 89D61CB2
DD046EE3 0E3FFD20 F9A45BBD F6413D58 3A2DBF59 924FD35C

QeU_y is
00F6 B632D194 C0388E22 D8437E55 8C552AE1
95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4

deV is
00CE E3480D86 45A17D24 9F2776D2 8BAE6169
52D1791F DB4B70F7 C3378732 AA1B2292 8448BCD1 DC2496D4
35B01048 066EBE4F 72903C36 1B1A9DC1 193DC2C9 D0891B96

QeV_x is
010E BFAFC6E8 5E08D24B FFFCC1A4 511DB0E6
34BEEB1B 6DEC8C59 39AE4476 6201AF62 00430BA9 7C8AC6A0
E9F08B33 CE7E9FEE B5BA4EE5 E0D81510 C24295B8 A08D0235

QeV_y is
00A4 A6EC300D F9E257B0 372B5E7A BFEF0934
36719A77 887EBB0B 18CF8099 B9F4212B 6E30A141 9C18E029
D36863CC 9D448F4D BA4D2A0E 60711BE5 72915FBD 4FEF2695

---

no Key Confirmation
Zs is
0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4

Ze is
00CD EA89621C FA46B132 F9E4CFE2 261CDE2D
4368EB56 56634C7C C98C7A00 CDE54ED1 866A0DD3 E6126C9D
2F845DAF F82CEB1D A08F5D87 521BB0EB ECA77911 169C20CC

```
Z is
                                  00CDEA89 621CFA46 B132F9E4
        CFE2261C DE2D4368 EB565663 4C7CC98C 7A00CDE5 4ED1866A
        0DD3E612 6C9D2F84 5DAFF82C EB1DA08F 5D87521B B0EBECA7
        7911169C 20CC0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                              2D4A46A1 7099BAA8
        330BC59D 4A1CF5AE 3A3075B4 C62BB26E 7FC98924 726D274C
        09646F44 08E6858C 43B42DAE D015EF26 1708D55E F24DAA7D
        3EA3D1C4 A08CFD24 DB6000A5 B8A67DE7 46F3D3F4 FF348515
        8FD3B691 55791DF4 6747D4DB BE17C4B5 58462E26 BE5ED35F
        E680E297 1422C3B0 1B17E167 FC437F84 869D8549 537B3338


KeyData is
                                              2D4A46A1 7099BAA8
        330BC59D 4A1CF5AE 3A3075B4 C62BB26E 7FC98924 726D274C
        09646F44 08E6858C 43B42DAE D015EF26 1708D55E F24DAA7D
        3EA3D1C4 A08CFD24 DB6000A5 B8A67DE7 46F3D3F4 FF348515
        8FD3B691 55791DF4 6747D4DB BE17C4B5 58462E26 BE5ED35F
        E680E297 1422C3B0 1B17E167 FC437F84 869D8549 537B3338




-----------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Zs is
                     0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


Ze is
                     00CD EA89621C FA46B132 F9E4CFE2 261CDE2D
        4368EB56 56634C7C C98C7A00 CDE54ED1 866A0DD3 E6126C9D
        2F845DAF F82CEB1D A08F5D87 521BB0EB ECA77911 169C20CC
```

Z is
                                00CDEA89 621CFA46 B132F9E4
        CFE2261C DE2D4368 EB565663 4C7CC98C 7A00CDE5 4ED1866A
        0DD3E612 6C9D2F84 5DAFF82C EB1DA08F 5D87521B B0EBECA7
        7911169C 20CC0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                        2D4A46A1 7099BAA8 330BC59D 4A1CF5AE
        3A3075B4 C62BB26E 7FC98924 726D274C 09646F44 08E6858C
        43B42DAE D015EF26 1708D55E F24DAA7D 3EA3D1C4 A08CFD24
        DB6000A5 B8A67DE7 46F3D3F4 FF348515 8FD3B691 55791DF4
        6747D4DB BE17C4B5 58462E26 BE5ED35F E680E297 1422C3B0
        1B17E167 FC437F84 869D8549 537B3338 50F0B78E 5CAD4ED6
        E0635DAE 1DCCA0EB 448F3BD1 3A0CDDB9 BE162CDF 3EF23175

MacData is
                        4B435F31 5F55414C 49434542 4F424259
        01EBB34D D75721AB F8ADC9DB ED17889C BB9765D9 0A7C60F2
        CEF007BB 0F2B26E1 4881FD44 42E689D6 1CB2DD04 6EE30E3F
        FD20F9A4 5BBDF641 3D583A2D BF59924F D35C00F6 B632D194
        C0388E22 D8437E55 8C552AE1 95ADFD15 3F92D749 08351B2F
        8C4EDA94 EDB0916D 1B53C020 B5EECAED 1A5FC38A 233E4830
        587BB2EE 3489B3B4 2A5A86A4 010EBFAF C6E85E08 D24BFFFC
        C1A4511D B0E634BE EB1B6DEC 8C5939AE 44766201 AF620043
        0BA97C8A C6A0E9F0 8B33CE7E 9FEEB5BA 4EE5E0D8 1510C242
        95B8A08D 023500A4 A6EC300D F9E257B0 372B5E7A BFEF0934
        36719A77 887EBB0B 18CF8099 B9F4212B 6E30A141 9C18E029
        D36863CC 9D448F4D BA4D2A0E 60711BE5 72915FBD 4FEF2695

MacKey is
                                                2D4A46A1 7099BAA8
        330BC59D 4A1CF5AE 3A3075B4 C62BB26E 7FC98924 726D274C

Mtag is
                        39AB0A29 E9A2E245 D6897BF7 CF51D6ED

```
        7AA59EBE E1E86820 F96B1804 1B158070 6D1911FA CDCCC8B6
        5B1328BD C0EB6AE0 F2C91A0C B53CDBBE 0D298A54 413D49F2


KeyData is
                                            09646F44 08E6858C
        43B42DAE D015EF26 1708D55E F24DAA7D 3EA3D1C4 A08CFD24
        DB6000A5 B8A67DE7 46F3D3F4 FF348515 8FD3B691 55791DF4
        6747D4DB BE17C4B5 58462E26 BE5ED35F E680E297 1422C3B0
        1B17E167 FC437F84 869D8549 537B3338 50F0B78E 5CAD4ED6
        E0635DAE 1DCCA0EB 448F3BD1 3A0CDDB9 BE162CDF 3EF23175




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Zs is
                    0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


Ze is
                    00CD EA89621C FA46B132 F9E4CFE2 261CDE2D
        4368EB56 56634C7C C98C7A00 CDE54ED1 866A0DD3 E6126C9D
        2F845DAF F82CEB1D A08F5D87 521BB0EB ECA77911 169C20CC


Z is
                                00CDEA89 621CFA46 B132F9E4
        CFE2261C DE2D4368 EB565663 4C7CC98C 7A00CDE5 4ED1866A
        0DD3E612 6C9D2F84 5DAFF82C EB1DA08F 5D87521B B0EBECA7
        7911169C 20CC0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                          2D4A46A1 7099BAA8 330BC59D 4A1CF5AE
        3A3075B4 C62BB26E 7FC98924 726D274C 09646F44 08E6858C
        43B42DAE D015EF26 1708D55E F24DAA7D 3EA3D1C4 A08CFD24
```

```
        DB6000A5 B8A67DE7 46F3D3F4 FF348515 8FD3B691 55791DF4
        6747D4DB BE17C4B5 58462E26 BE5ED35F E680E297 1422C3B0
        1B17E167 FC437F84 869D8549 537B3338 50F0B78E 5CAD4ED6
        E0635DAE 1DCCA0EB 448F3BD1 3A0CDDB9 BE162CDF 3EF23175


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        010EBFAF C6E85E08 D24BFFFC C1A4511D B0E634BE EB1B6DEC
        8C5939AE 44766201 AF620043 0BA97C8A C6A0E9F0 8B33CE7E
        9FEEB5BA 4EE5E0D8 1510C242 95B8A08D 023500A4 A6EC300D
        F9E257B0 372B5E7A BFEF0934 36719A77 887EBB0B 18CF8099
        B9F4212B 6E30A141 9C18E029 D36863CC 9D448F4D BA4D2A0E
        60711BE5 72915FBD 4FEF2695 01EBB34D D75721AB F8ADC9DB
        ED17889C BB9765D9 0A7C60F2 CEF007BB 0F2B26E1 4881FD44
        42E689D6 1CB2DD04 6EE30E3F FD20F9A4 5BBDF641 3D583A2D
        BF59924F D35C00F6 B632D194 C0388E22 D8437E55 8C552AE1
        95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
        B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4


MacKey is
                                             2D4A46A1 7099BAA8
        330BC59D 4A1CF5AE 3A3075B4 C62BB26E 7FC98924 726D274C


Mtag is
                         1F9E2BC0 F3AE6550 53D3A462 B5EB9333
        BDB8BCB3 1E193748 EAA73689 A1BD5649 F6612926 6F097365
        74ACD563 3157F95C 6B9636FB 721A9BFB 08E91A8C 74CD324D


KeyData is
                                             09646F44 08E6858C
        43B42DAE D015EF26 1708D55E F24DAA7D 3EA3D1C4 A08CFD24
        DB6000A5 B8A67DE7 46F3D3F4 FF348515 8FD3B691 55791DF4
        6747D4DB BE17C4B5 58462E26 BE5ED35F E680E297 1422C3B0
        1B17E167 FC437F84 869D8549 537B3338 50F0B78E 5CAD4ED6
        E0635DAE 1DCCA0EB 448F3BD1 3A0CDDB9 BE162CDF 3EF23175




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
Zs is
```

```
                    0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
         3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
         F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


Ze is
                    00CD EA89621C FA46B132 F9E4CFE2 261CDE2D
         4368EB56 56634C7C C98C7A00 CDE54ED1 866A0DD3 E6126C9D
         2F845DAF F82CEB1D A08F5D87 521BB0EB ECA77911 169C20CC


Z is
                                   00CDEA89 621CFA46 B132F9E4
         CFE2261C DE2D4368 EB565663 4C7CC98C 7A00CDE5 4ED1866A
         0DD3E612 6C9D2F84 5DAFF82C EB1DA08F 5D87521B B0EBECA7
         7911169C 20CC0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
         3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
         F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


OtherInfo is
         12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                           2D4A46A1 7099BAA8 330BC59D 4A1CF5AE
         3A3075B4 C62BB26E 7FC98924 726D274C 09646F44 08E6858C
         43B42DAE D015EF26 1708D55E F24DAA7D 3EA3D1C4 A08CFD24
         DB6000A5 B8A67DE7 46F3D3F4 FF348515 8FD3B691 55791DF4
         6747D4DB BE17C4B5 58462E26 BE5ED35F E680E297 1422C3B0
         1B17E167 FC437F84 869D8549 537B3338 50F0B78E 5CAD4ED6
         E0635DAE 1DCCA0EB 448F3BD1 3A0CDDB9 BE162CDF 3EF23175


U2V
----------------
MacData is
                           4B435F32 5F55414C 49434542 4F424259
         01EBB34D D75721AB F8ADC9DB ED17889C BB9765D9 0A7C60F2
         CEF007BB 0F2B26E1 4881FD44 42E689D6 1CB2DD04 6EE30E3F
         FD20F9A4 5BBDF641 3D583A2D BF59924F D35C00F6 B632D194
         C0388E22 D8437E55 8C552AE1 95ADFD15 3F92D749 08351B2F
         8C4EDA94 EDB0916D 1B53C020 B5EECAED 1A5FC38A 233E4830
         587BB2EE 3489B3B4 2A5A86A4 010EBFAF C6E85E08 D24BFFFC
         C1A4511D B0E634BE EB1B6DEC 8C5939AE 44766201 AF620043
         0BA97C8A C6A0E9F0 8B33CE7E 9FEEB5BA 4EE5E0D8 1510C242
```

95B8A08D 023500A4 A6EC300D F9E257B0 372B5E7A BFEF0934
36719A77 887EBB0B 18CF8099 B9F4212B 6E30A141 9C18E029
D36863CC 9D448F4D BA4D2A0E 60711BE5 72915FBD 4FEF2695

MacKey is
2D4A46A1 7099BAA8
330BC59D 4A1CF5AE 3A3075B4 C62BB26E 7FC98924 726D274C

Mtag is
332623B6 15C0AF2C EF5C1D66 70670B3E
6D01479C EF6041AD 617A5DA9 53E6211F 89E98E1A F3002302
817FAE27 6E92547F 79266D58 82B7732D 6B46A203 08445842

V2U

MacData is
4B435F32 5F56424F 42425941 4C494345
010EBFAF C6E85E08 D24BFFFC C1A4511D B0E634BE EB1B6DEC
8C5939AE 44766201 AF620043 0BA97C8A C6A0E9F0 8B33CE7E
9FEEB5BA 4EE5E0D8 1510C242 95B8A08D 023500A4 A6EC300D
F9E257B0 372B5E7A BFEF0934 36719A77 887EBB0B 18CF8099
B9F4212B 6E30A141 9C18E029 D36863CC 9D448F4D BA4D2A0E
60711BE5 72915FBD 4FEF2695 01EBB34D D75721AB F8ADC9DB
ED17889C BB9765D9 0A7C60F2 CEF007BB 0F2B26E1 4881FD44
42E689D6 1CB2DD04 6EE30E3F FD20F9A4 5BBDF641 3D583A2D
BF59924F D35C00F6 B632D194 C0388E22 D8437E55 8C552AE1
95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4

MacKey is
2D4A46A1 7099BAA8
330BC59D 4A1CF5AE 3A3075B4 C62BB26E 7FC98924 726D274C

Mtag is
F752AFAE F5E2F786 008BA46F 9524516B
D4F80388 C35FB7A5 CEA8F38A EEDAED09 AABFC450 2EC99150
F53C2FC8 791FB613 FCE28F7E 97FC1C65 17CC8A4F 803209F9

KeyData is
09646F44 08E6858C

```
        43B42DAE D015EF26 1708D55E F24DAA7D 3EA3D1C4 A08CFD24
        DB6000A5 B8A67DE7 46F3D3F4 FF348515 8FD3B691 55791DF4
        6747D4DB BE17C4B5 58462E26 BE5ED35F E680E297 1422C3B0
        1B17E167 FC437F84 869D8549 537B3338 50F0B78E 5CAD4ED6
        E0635DAE 1DCCA0EB 448F3BD1 3A0CDDB9 BE162CDF 3EF23175



FullMQV(P-521)
-------------------------------------------------------------
dsU is
                    017D 1527DCC7 C046E4D3 04600ED0 D3A625F6
        AA46C475 14D92CB6 A6416C1B 8978B3E6 E9796830 6FFC49D0
        0371CCBD 4B796AA3 6547A6ED 3E78BBDF F2CFF34C E4C57FC9


QsU_x is
                    00D0 C2D9A667 F85A3C27 0C838535 04616791
        F3052858 3CF2D5CD D35D4E77 D440FE51 01DFC0E1 953983A9
        C1D7C330 7E6213FB CEB3D113 460D7B45 BBACAE5D 54B68166


QsU_y is
                    01C8 A85F0367 B3B1F4DE 8A74021E 08E13EA5
        65EF012E 647DD317 3B21DD6B B9987155 73063EBB 3152CAA7
        91ABD47F D31FB528 799413F8 DFF76E28 64E9870A 262ECACB


dsV is
                    00A0 752E306C ECD87AB0 E4830DA1 44F8038C
        E7B8C2B3 E5422ACF 9AAA6CCF 21818316 9A4CCA2A D577A64E
        6D86DCBF F5C1727A 11FD1CB8 E3A53842 B84005FD A9AC7F36


QsV_x is
                    0128 C16B23A4 259C9FE4 257C1DA4 3C7735C4
        3337929E 0FD86CC2 A778975B 67184CC2 825F6E66 7876D404
        BBF03E04 1F8FAD2F CCC036CD 5448B64E 9BD7DF6F 537659BB


QsV_y is
                    0108 089A6431 FED52344 DD5859A0 E5432D16
        9BEE36F5 3F857AED 08A69FE3 07B1C94B 8ABDCF65 0C4D1297
        29D69FB7 7D1CC1CD 651C676B 309CE018 C9771EAB 9CA5A754
```

```
deU is
                    0113 F82DA825 735E3D97 276683B2 B74277BA
        D27335EA 71664AF2 430CC4F3 3459B966 9EE78B3F FB9B8683
        015D344D CBFEF6FB 9AF4C6C4 70BE2545 16CD3C1A 1FB47362


QeU_x is
                    01EB B34DD757 21ABF8AD C9DBED17 889CBB97
        65D90A7C 60F2CEF0 07BB0F2B 26E14881 FD4442E6 89D61CB2
        DD046EE3 0E3FFD20 F9A45BBD F6413D58 3A2DBF59 924FD35C


QeU_y is
                    00F6 B632D194 C0388E22 D8437E55 8C552AE1
        95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
        B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4


deV is
                    00CE E3480D86 45A17D24 9F2776D2 8BAE6169
        52D1791F DB4B70F7 C3378732 AA1B2292 8448BCD1 DC2496D4
        35B01048 066EBE4F 72903C36 1B1A9DC1 193DC2C9 D0891B96


QeV_x is
                    010E BFAFC6E8 5E08D24B FFFCC1A4 511DB0E6
        34BEEB1B 6DEC8C59 39AE4476 6201AF62 00430BA9 7C8AC6A0
        E9F08B33 CE7E9FEE B5BA4EE5 E0D81510 C24295B8 A08D0235


QeV_y is
                    00A4 A6EC300D F9E257B0 372B5E7A BFEF0934
        36719A77 887EBB0B 18CF8099 B9F4212B 6E30A141 9C18E029
        D36863CC 9D448F4D BA4D2A0E 60711BE5 72915FBD 4FEF2695




------------------------------------------------------------
no Key Confirmation
Z is
                    01BE 3D4F8058 EF18D790 2A263CEF 57325EAE
        C9B9D6D6 411800FA 0518A173 DA7AEC8E 984B2AFA 782C2506
        639AFB54 092D56E1 2C02AE2B 943B22C3 8763DBC7 DE3BDFC1
```

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                            E7946061 588EA80B
        9FE8FF31 515B007B 12EE2988 633DE0ED 71EBCD33 B605F8C2
        EAD28CBC D07BAA3D FFCC7BA3 51860A90 D8E28699 BCF1866D
        46CBC313 01CBBB2B C44125FC B6B5B974 E59B2010 90898AC1
        511261EB 392EBD23 53B7A3EA 65F1CF67 54BB5519 C190C47D
        8AE32B51 78293EBA 66C7E633 BACEF480 9A349F0C 1663EADC


KeyData is
                                            E7946061 588EA80B
        9FE8FF31 515B007B 12EE2988 633DE0ED 71EBCD33 B605F8C2
        EAD28CBC D07BAA3D FFCC7BA3 51860A90 D8E28699 BCF1866D
        46CBC313 01CBBB2B C44125FC B6B5B974 E59B2010 90898AC1
        511261EB 392EBD23 53B7A3EA 65F1CF67 54BB5519 C190C47D
        8AE32B51 78293EBA 66C7E633 BACEF480 9A349F0C 1663EADC




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Z is
                    01BE 3D4F8058 EF18D790 2A263CEF 57325EAE
        C9B9D6D6 411800FA 0518A173 DA7AEC8E 984B2AFA 782C2506
        639AFB54 092D56E1 2C02AE2B 943B22C3 8763DBC7 DE3BDFC1


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                          E7946061 588EA80B 9FE8FF31 515B007B
        12EE2988 633DE0ED 71EBCD33 B605F8C2 EAD28CBC D07BAA3D
        FFCC7BA3 51860A90 D8E28699 BCF1866D 46CBC313 01CBBB2B
        C44125FC B6B5B974 E59B2010 90898AC1 511261EB 392EBD23
        53B7A3EA 65F1CF67 54BB5519 C190C47D 8AE32B51 78293EBA
        66C7E633 BACEF480 9A349F0C 1663EADC 73A64A8A EF283A37
        E0CA305E 0A9124D7 221F5D67 3DDB7B12 CB0A8516 9BFD17C9
```

MacData is
                        4B435F31 5F55414C 49434542 4F424259
        01EBB34D D75721AB F8ADC9DB ED17889C BB9765D9 0A7C60F2
        CEF007BB 0F2B26E1 4881FD44 42E689D6 1CB2DD04 6EE30E3F
        FD20F9A4 5BBDF641 3D583A2D BF59924F D35C00F6 B632D194
        C0388E22 D8437E55 8C552AE1 95ADFD15 3F92D749 08351B2F
        8C4EDA94 EDB0916D 1B53C020 B5EECAED 1A5FC38A 233E4830
        587BB2EE 3489B3B4 2A5A86A4 010EBFAF C6E85E08 D24BFFFC
        C1A4511D B0E634BE EB1B6DEC 8C5939AE 44766201 AF620043
        0BA97C8A C6A0E9F0 8B33CE7E 9FEEB5BA 4EE5E0D8 1510C242
        95B8A08D 023500A4 A6EC300D F9E257B0 372B5E7A BFEF0934
        36719A77 887EBB0B 18CF8099 B9F4212B 6E30A141 9C18E029
        D36863CC 9D448F4D BA4D2A0E 60711BE5 72915FBD 4FEF2695

MacKey is
                                            E7946061 588EA80B
        9FE8FF31 515B007B 12EE2988 633DE0ED 71EBCD33 B605F8C2

Mtag is
                        8AA7CAEA EC472789 1C57399C 291BC2E1
        538A85DC EC4BC42E 9C48B37C 3F42B4E5 2FB2F152 A655D1A7
        33F3D43D A91EA799 952B197F DF6E8DF8 6CD1FE47 09E1AE15

KeyData is
                                            EAD28CBC D07BAA3D
        FFCC7BA3 51860A90 D8E28699 BCF1866D 46CBC313 01CBBB2B
        C44125FC B6B5B974 E59B2010 90898AC1 511261EB 392EBD23
        53B7A3EA 65F1CF67 54BB5519 C190C47D 8AE32B51 78293EBA
        66C7E633 BACEF480 9A349F0C 1663EADC 73A64A8A EF283A37
        E0CA305E 0A9124D7 221F5D67 3DDB7B12 CB0A8516 9BFD17C9

Scheme Responder, Key Confirmation Provider: V to U
Z is
                    01BE 3D4F8058 EF18D790 2A263CEF 57325EAE
        C9B9D6D6 411800FA 0518A173 DA7AEC8E 984B2AFA 782C2506
        639AFB54 092D56E1 2C02AE2B 943B22C3 8763DBC7 DE3BDFC1

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         E7946061 588EA80B 9FE8FF31 515B007B
        12EE2988 633DE0ED 71EBCD33 B605F8C2 EAD28CBC D07BAA3D
        FFCC7BA3 51860A90 D8E28699 BCF1866D 46CBC313 01CBBB2B
        C44125FC B6B5B974 E59B2010 90898AC1 511261EB 392EBD23
        53B7A3EA 65F1CF67 54BB5519 C190C47D 8AE32B51 78293EBA
        66C7E633 BACEF480 9A349F0C 1663EADC 73A64A8A EF283A37
        E0CA305E 0A9124D7 221F5D67 3DDB7B12 CB0A8516 9BFD17C9


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        010EBFAF C6E85E08 D24BFFFC C1A4511D B0E634BE EB1B6DEC
        8C5939AE 44766201 AF620043 0BA97C8A C6A0E9F0 8B33CE7E
        9FEEB5BA 4EE5E0D8 1510C242 95B8A08D 023500A4 A6EC300D
        F9E257B0 372B5E7A BFEF0934 36719A77 887EBB0B 18CF8099
        B9F4212B 6E30A141 9C18E029 D36863CC 9D448F4D BA4D2A0E
        60711BE5 72915FBD 4FEF2695 01EBB34D D75721AB F8ADC9DB
        ED17889C BB9765D9 0A7C60F2 CEF007BB 0F2B26E1 4881FD44
        42E689D6 1CB2DD04 6EE30E3F FD20F9A4 5BBDF641 3D583A2D
        BF59924F D35C00F6 B632D194 C0388E22 D8437E55 8C552AE1
        95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
        B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4


MacKey is
                                                 E7946061 588EA80B
        9FE8FF31 515B007B 12EE2988 633DE0ED 71EBCD33 B605F8C2


Mtag is
                         94CDE460 990F798F 070120D1 1E84893F
        75A6E8DD 3BF7ED88 A37BA3DF AEBEBC2C 63E6A3FC BA69C41A
        F8F0B6E8 342B9578 E4475B71 DBC92F2E 47BCFD6A C397DF05


KeyData is
                                                 EAD28CBC D07BAA3D
        FFCC7BA3 51860A90 D8E28699 BCF1866D 46CBC313 01CBBB2B
        C44125FC B6B5B974 E59B2010 90898AC1 511261EB 392EBD23
        53B7A3EA 65F1CF67 54BB5519 C190C47D 8AE32B51 78293EBA
        66C7E633 BACEF480 9A349F0C 1663EADC 73A64A8A EF283A37
```

E0CA305E 0A9124D7 221F5D67 3DDB7B12 CB0A8516 9BFD17C9

Scheme Initiator, Key Confirmation Bilateral
Z is
01BE 3D4F8058 EF18D790 2A263CEF 57325EAE
C9B9D6D6 411800FA 0518A173 DA7AEC8E 984B2AFA 782C2506
639AFB54 092D56E1 2C02AE2B 943B22C3 8763DBC7 DE3BDFC1

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
E7946061 588EA80B 9FE8FF31 515B007B
12EE2988 633DE0ED 71EBCD33 B605F8C2 EAD28CBC D07BAA3D
FFCC7BA3 51860A90 D8E28699 BCF1866D 46CBC313 01CBBB2B
C44125FC B6B5B974 E59B2010 90898AC1 511261EB 392EBD23
53B7A3EA 65F1CF67 54BB5519 C190C47D 8AE32B51 78293EBA
66C7E633 BACEF480 9A349F0C 1663EADC 73A64A8A EF283A37
E0CA305E 0A9124D7 221F5D67 3DDB7B12 CB0A8516 9BFD17C9

U2V

MacData is
4B435F32 5F55414C 49434542 4F424259
01EBB34D D75721AB F8ADC9DB ED17889C BB9765D9 0A7C60F2
CEF007BB 0F2B26E1 4881FD44 42E689D6 1CB2DD04 6EE30E3F
FD20F9A4 5BBDF641 3D583A2D BF59924F D35C00F6 B632D194
C0388E22 D8437E55 8C552AE1 95ADFD15 3F92D749 08351B2F
8C4EDA94 EDB0916D 1B53C020 B5EECAED 1A5FC38A 233E4830
587BB2EE 3489B3B4 2A5A86A4 010EBFAF C6E85E08 D24BFFFC
C1A4511D B0E634BE EB1B6DEC 8C5939AE 44766201 AF620043
0BA97C8A C6A0E9F0 8B33CE7E 9FEEB5BA 4EE5E0D8 1510C242
95B8A08D 023500A4 A6EC300D F9E257B0 372B5E7A BFEF0934
36719A77 887EBB0B 18CF8099 B9F4212B 6E30A141 9C18E029
D36863CC 9D448F4D BA4D2A0E 60711BE5 72915FBD 4FEF2695

MacKey is

```
                                                E7946061 588EA80B
        9FE8FF31 515B007B 12EE2988 633DE0ED 71EBCD33 B605F8C2


Mtag is
                        929585B7 A0144071 35759347 4CA4B4DC
        9A56DD61 4F15400C EB305EFE 84C0BA0B 2D2BB87C AF153EBC
        7105AB31 59E7B7AD 1FA69669 7C137B56 2AD8C314 5E3B2730


V2U
----------------
MacData is
                        4B435F32 5F56424F 42425941 4C494345
        010EBFAF C6E85E08 D24BFFFC C1A4511D B0E634BE EB1B6DEC
        8C5939AE 44766201 AF620043 0BA97C8A C6A0E9F0 8B33CE7E
        9FEEB5BA 4EE5E0D8 1510C242 95B8A08D 023500A4 A6EC300D
        F9E257B0 372B5E7A BFEF0934 36719A77 887EBB0B 18CF8099
        B9F4212B 6E30A141 9C18E029 D36863CC 9D448F4D BA4D2A0E
        60711BE5 72915FBD 4FEF2695 01EBB34D D75721AB F8ADC9DB
        ED17889C BB9765D9 0A7C60F2 CEF007BB 0F2B26E1 4881FD44
        42E689D6 1CB2DD04 6EE30E3F FD20F9A4 5BBDF641 3D583A2D
        BF59924F D35C00F6 B632D194 C0388E22 D8437E55 8C552AE1
        95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
        B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4


MacKey is
                                                E7946061 588EA80B
        9FE8FF31 515B007B 12EE2988 633DE0ED 71EBCD33 B605F8C2


Mtag is
                        CC624E00 604233DA A807A33C 0662C7D4
        91317C12 F079851F 3805F602 11EEAFB5 E986E2A2 DD422259
        B7A9E32C 68C8AC9E 1BA7F641 04E70399 BAE6FA39 4F4E5896


KeyData is
                                                EAD28CBC D07BAA3D
        FFCC7BA3 51860A90 D8E28699 BCF1866D 46CBC313 01CBBB2B
        C44125FC B6B5B974 E59B2010 90898AC1 511261EB 392EBD23
        53B7A3EA 65F1CF67 54BB5519 C190C47D 8AE32B51 78293EBA
        66C7E633 BACEF480 9A349F0C 1663EADC 73A64A8A EF283A37
        E0CA305E 0A9124D7 221F5D67 3DDB7B12 CB0A8516 9BFD17C9
```

EphemeralUnifiedCDH(P-521)
---
deU is
0113 F82DA825 735E3D97 276683B2 B74277BA
D27335EA 71664AF2 430CC4F3 3459B966 9EE78B3F FB9B8683
015D344D CBFEF6FB 9AF4C6C4 70BE2545 16CD3C1A 1FB47362

QeU_x is
01EB B34DD757 21ABF8AD C9DBED17 889CBB97
65D90A7C 60F2CEF0 07BB0F2B 26E14881 FD4442E6 89D61CB2
DD046EE3 0E3FFD20 F9A45BBD F6413D58 3A2DBF59 924FD35C

QeU_y is
00F6 B632D194 C0388E22 D8437E55 8C552AE1
95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4

deV is
00CE E3480D86 45A17D24 9F2776D2 8BAE6169
52D1791F DB4B70F7 C3378732 AA1B2292 8448BCD1 DC2496D4
35B01048 066EBE4F 72903C36 1B1A9DC1 193DC2C9 D0891B96

QeV_x is
010E BFAFC6E8 5E08D24B FFFCC1A4 511DB0E6
34BEEB1B 6DEC8C59 39AE4476 6201AF62 00430BA9 7C8AC6A0
E9F08B33 CE7E9FEE B5BA4EE5 E0D81510 C24295B8 A08D0235

QeV_y is
00A4 A6EC300D F9E257B0 372B5E7A BFEF0934
36719A77 887EBB0B 18CF8099 B9F4212B 6E30A141 9C18E029
D36863CC 9D448F4D BA4D2A0E 60711BE5 72915FBD 4FEF2695

---
no Key Confirmation
Z is

```
                    00CD EA89621C FA46B132 F9E4CFE2 261CDE2D
        4368EB56 56634C7C C98C7A00 CDE54ED1 866A0DD3 E6126C9D
        2F845DAF F82CEB1D A08F5D87 521BB0EB ECA77911 169C20CC


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                            C642987D 025C5B37
        80D9CC99 82B785B2 CCD78A16 20B41B83 3B78F149 FE823A23
        CE7B2712 7E8E07A1 F4CC7D1C E5D8849D FC82B411 BACBC476
        B2E0C1A8 9025A16E 45956081 87DC2F82 CCC4C5E3 FC3504D8
        5BE8497A 2B240AAD 7A5ACA6C 42691F08 9F9D072A 0A66CF43
        BBEB5F84 13D923C9 F77515E5 8E5989F3 7D09E6D2 922C2B57


KeyData is
                                            C642987D 025C5B37
        80D9CC99 82B785B2 CCD78A16 20B41B83 3B78F149 FE823A23
        CE7B2712 7E8E07A1 F4CC7D1C E5D8849D FC82B411 BACBC476
        B2E0C1A8 9025A16E 45956081 87DC2F82 CCC4C5E3 FC3504D8
        5BE8497A 2B240AAD 7A5ACA6C 42691F08 9F9D072A 0A66CF43
        BBEB5F84 13D923C9 F77515E5 8E5989F3 7D09E6D2 922C2B57




OnePassUnifiedCDH(P-521)
-----------------------------------------------------------
dsU is
                    017D 1527DCC7 C046E4D3 04600ED0 D3A625F6
        AA46C475 14D92CB6 A6416C1B 8978B3E6 E9796830 6FFC49D0
        0371CCBD 4B796AA3 6547A6ED 3E78BBDF F2CFF34C E4C57FC9


QsU_x is
                    00D0 C2D9A667 F85A3C27 0C838535 04616791
        F3052858 3CF2D5CD D35D4E77 D440FE51 01DFC0E1 953983A9
        C1D7C330 7E6213FB CEB3D113 460D7B45 BBACAE5D 54B68166


QsU_y is
                    01C8 A85F0367 B3B1F4DE 8A74021E 08E13EA5
        65EF012E 647DD317 3B21DD6B B9987155 73063EBB 3152CAA7
```

91ABD47F D31FB528 799413F8 DFF76E28 64E9870A 262ECACB

dsV is
00A0 752E306C ECD87AB0 E4830DA1 44F8038C
E7B8C2B3 E5422ACF 9AAA6CCF 21818316 9A4CCA2A D577A64E
6D86DCBF F5C1727A 11FD1CB8 E3A53842 B84005FD A9AC7F36

QsV_x is
0128 C16B23A4 259C9FE4 257C1DA4 3C7735C4
3337929E 0FD86CC2 A778975B 67184CC2 825F6E66 7876D404
BBF03E04 1F8FAD2F CCC036CD 5448B64E 9BD7DF6F 537659BB

QsV_y is
0108 089A6431 FED52344 DD5859A0 E5432D16
9BEE36F5 3F857AED 08A69FE3 07B1C94B 8ABDCF65 0C4D1297
29D69FB7 7D1CC1CD 651C676B 309CE018 C9771EAB 9CA5A754

deU is
0113 F82DA825 735E3D97 276683B2 B74277BA
D27335EA 71664AF2 430CC4F3 3459B966 9EE78B3F FB9B8683
015D344D CBFEF6FB 9AF4C6C4 70BE2545 16CD3C1A 1FB47362

QeU_x is
01EB B34DD757 21ABF8AD C9DBED17 889CBB97
65D90A7C 60F2CEF0 07BB0F2B 26E14881 FD4442E6 89D61CB2
DD046EE3 0E3FFD20 F9A45BBD F6413D58 3A2DBF59 924FD35C

QeU_y is
00F6 B632D194 C0388E22 D8437E55 8C552AE1
95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4

---

no Key Confirmation
Zs is
0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1

```
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


Ze is
                    0104 F83D9416 E8BB0FEB CBAC67FE CA3F23A1
        54E9ECE9 CE152A38 1308754A E68B575A 67D0BA3E 7FAB218C
        74C58BEF DB2E494D 510158A2 5EF077C1 D1C89E58 5F1C44F7


Z is
                                  0104F83D 9416E8BB 0FEBCBAC
        67FECA3F 23A154E9 ECE9CE15 2A381308 754AE68B 575A67D0
        BA3E7FAB 218C74C5 8BEFDB2E 494D5101 58A25EF0 77C1D1C8
        9E585F1C 44F70138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                             A649B1A5 7457DCB4
        15134A13 B4D9973D 13E48BA9 3B22A7A1 ED9F09EA BB493978
        A5E301CF 7FCF1D12 37E26111 8CBED7AD E92EF2ED 856A6309
        3182B539 40BE7572 E914505F A51461C4 F4B889C0 8BFB0442
        0C994ED1 05EB68B9 8EAF6E42 41E84F8F 3A4C8BF8 A62B694F
        05FC5338 65A7B6AB EEC2D8A2 25019C14 6B17A14E AB572BD0


KeyData is
                                             A649B1A5 7457DCB4
        15134A13 B4D9973D 13E48BA9 3B22A7A1 ED9F09EA BB493978
        A5E301CF 7FCF1D12 37E26111 8CBED7AD E92EF2ED 856A6309
        3182B539 40BE7572 E914505F A51461C4 F4B889C0 8BFB0442
        0C994ED1 05EB68B9 8EAF6E42 41E84F8F 3A4C8BF8 A62B694F
        05FC5338 65A7B6AB EEC2D8A2 25019C14 6B17A14E AB572BD0




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                    0020 905F7F3A 0298275E 33482000 1D90F0B2
```

```
        F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
        9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D


Zs is
                    0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


Ze is
                    0104 F83D9416 E8BB0FEB CBAC67FE CA3F23A1
        54E9ECE9 CE152A38 1308754A E68B575A 67D0BA3E 7FAB218C
        74C58BEF DB2E494D 510158A2 5EF077C1 D1C89E58 5F1C44F7


Z is
                                  0104F83D 9416E8BB 0FEBCBAC
        67FECA3F 23A154E9 ECE9CE15 2A381308 754AE68B 575A67D0
        BA3E7FAB 218C74C5 8BEFDB2E 494D5101 58A25EF0 77C1D1C8
        9E585F1C 44F70138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         A649B1A5 7457DCB4 15134A13 B4D9973D
        13E48BA9 3B22A7A1 ED9F09EA BB493978 A5E301CF 7FCF1D12
        37E26111 8CBED7AD E92EF2ED 856A6309 3182B539 40BE7572
        E914505F A51461C4 F4B889C0 8BFB0442 0C994ED1 05EB68B9
        8EAF6E42 41E84F8F 3A4C8BF8 A62B694F 05FC5338 65A7B6AB
        EEC2D8A2 25019C14 6B17A14E AB572BD0 B3A85D44 9099783D
        4F192877 B712A0BD 12B53459 A8342F13 4D5C5717 AA34ECC5


MacData is
            4B43 5F315F55 414C4943 45424F42 425901EB B34DD757
        21ABF8AD C9DBED17 889CBB97 65D90A7C 60F2CEF0 07BB0F2B
        26E14881 FD4442E6 89D61CB2 DD046EE3 0E3FFD20 F9A45BBD
        F6413D58 3A2DBF59 924FD35C 00F6B632 D194C038 8E22D843
        7E558C55 2AE195AD FD153F92 D7490835 1B2F8C4E DA94EDB0
        916D1B53 C020B5EE CAED1A5F C38A233E 4830587B B2EE3489
```

B3B42A5A 86A40020 905F7F3A 0298275E 33482000 1D90F0B2
F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D

MacKey is
A649B1A5 7457DCB4
15134A13 B4D9973D 13E48BA9 3B22A7A1 ED9F09EA BB493978

Mtag is
BA11042B 74ED409A 83E73B0C A1C64A58
E07B31BA 35B86FEF 8B7AD787 F683F557 77EF0E35 04BEB56E
0FEB75BC 824428A6 775E5BB0 D29B0CC2 1BFC3B72 1D10DC55

KeyData is
A5E301CF 7FCF1D12
37E26111 8CBED7AD E92EF2ED 856A6309 3182B539 40BE7572
E914505F A51461C4 F4B889C0 8BFB0442 0C994ED1 05EB68B9
8EAF6E42 41E84F8F 3A4C8BF8 A62B694F 05FC5338 65A7B6AB
EEC2D8A2 25019C14 6B17A14E AB572BD0 B3A85D44 9099783D
4F192877 B712A0BD 12B53459 A8342F13 4D5C5717 AA34ECC5

Scheme Responder, Key Confirmation Provider: V to U
NonceU is
0020 905F7F3A 0298275E 33482000 1D90F0B2
F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D

Zs is
0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4

Ze is
0104 F83D9416 E8BB0FEB CBAC67FE CA3F23A1
54E9ECE9 CE152A38 1308754A E68B575A 67D0BA3E 7FAB218C
74C58BEF DB2E494D 510158A2 5EF077C1 D1C89E58 5F1C44F7

Z is
                                0104F83D 9416E8BB 0FEBCBAC
        67FECA3F 23A154E9 ECE9CE15 2A381308 754AE68B 575A67D0
        BA3E7FAB 218C74C5 8BEFDB2E 494D5101 58A25EF0 77C1D1C8
        9E585F1C 44F70138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                        A649B1A5 7457DCB4 15134A13 B4D9973D
        13E48BA9 3B22A7A1 ED9F09EA BB493978 A5E301CF 7FCF1D12
        37E26111 8CBED7AD E92EF2ED 856A6309 3182B539 40BE7572
        E914505F A51461C4 F4B889C0 8BFB0442 0C994ED1 05EB68B9
        8EAF6E42 41E84F8F 3A4C8BF8 A62B694F 05FC5338 65A7B6AB
        EEC2D8A2 25019C14 6B17A14E AB572BD0 B3A85D44 9099783D
        4F192877 B712A0BD 12B53459 A8342F13 4D5C5717 AA34ECC5

MacData is
                                                    4B435F31
        5F56424F 42425941 4C494345 01EBB34D D75721AB F8ADC9DB
        ED17889C BB9765D9 0A7C60F2 CEF007BB 0F2B26E1 4881FD44
        42E689D6 1CB2DD04 6EE30E3F FD20F9A4 5BBDF641 3D583A2D
        BF59924F D35C00F6 B632D194 C0388E22 D8437E55 8C552AE1
        95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
        B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4

MacKey is
                                                A649B1A5 7457DCB4
        15134A13 B4D9973D 13E48BA9 3B22A7A1 ED9F09EA BB493978

Mtag is
                        CB211DDE F1CADA90 2EC21C58 165E89AC
        D51FF0FB 8D42B87D 6BF20733 155C9F5A 1C48D948 0DDC1A81
        D53E3E1D 13EE9DFE BB2745C5 E2F42800 29309F5F 73C1DFD3

KeyData is

                                                A5E301CF 7FCF1D12
        37E26111 8CBED7AD E92EF2ED 856A6309 3182B539 40BE7572
        E914505F A51461C4 F4B889C0 8BFB0442 0C994ED1 05EB68B9
        8EAF6E42 41E84F8F 3A4C8BF8 A62B694F 05FC5338 65A7B6AB
        EEC2D8A2 25019C14 6B17A14E AB572BD0 B3A85D44 9099783D
        4F192877 B712A0BD 12B53459 A8342F13 4D5C5717 AA34ECC5

Scheme Initiator, Key Confirmation Bilateral
NonceV is
                    0020 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
        9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D

Zs is
                    0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4

Ze is
                    0104 F83D9416 E8BB0FEB CBAC67FE CA3F23A1
        54E9ECE9 CE152A38 1308754A E68B575A 67D0BA3E 7FAB218C
        74C58BEF DB2E494D 510158A2 5EF077C1 D1C89E58 5F1C44F7

Z is
                                    0104F83D 9416E8BB 0FEBCBAC
        67FECA3F 23A154E9 ECE9CE15 2A381308 754AE68B 575A67D0
        BA3E7FAB 218C74C5 8BEFDB2E 494D5101 58A25EF0 77C1D1C8
        9E585F1C 44F70138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                            A649B1A5 7457DCB4 15134A13 B4D9973D
        13E48BA9 3B22A7A1 ED9F09EA BB493978 A5E301CF 7FCF1D12

```
        37E26111 8CBED7AD E92EF2ED 856A6309 3182B539 40BE7572
        E914505F A51461C4 F4B889C0 8BFB0442 0C994ED1 05EB68B9
        8EAF6E42 41E84F8F 3A4C8BF8 A62B694F 05FC5338 65A7B6AB
        EEC2D8A2 25019C14 6B17A14E AB572BD0 B3A85D44 9099783D
        4F192877 B712A0BD 12B53459 A8342F13 4D5C5717 AA34ECC5


U2V
----------------
MacData is
            4B43 5F325F55 414C4943 45424F42 425901EB B34DD757
        21ABF8AD C9DBED17 889CBB97 65D90A7C 60F2CEF0 07BB0F2B
        26E14881 FD4442E6 89D61CB2 DD046EE3 0E3FFD20 F9A45BBD
        F6413D58 3A2DBF59 924FD35C 00F6B632 D194C038 8E22D843
        7E558C55 2AE195AD FD153F92 D7490835 1B2F8C4E DA94EDB0
        916D1B53 C020B5EE CAED1A5F C38A233E 4830587B B2EE3489
        B3B42A5A 86A40020 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
        9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D


MacKey is
                                               A649B1A5 7457DCB4
        15134A13 B4D9973D 13E48BA9 3B22A7A1 ED9F09EA BB493978


Mtag is
                         8D8FBD76 2F350C8D B1D5D6E9 3E259DAF
        69679568 275C55A7 E58076A7 2EF06D4C 02005E1E 4647B9E6
        716A9F4E CABC1E10 E91D1E2B 57D05DD4 132DB133 4945112C


V2U
----------------
MacData is
            4B43 5F325F56 424F4242 59414C49 43450020 905F7F3A
        0298275E 33482000 1D90F0B2 F19737D1 F8452AC5 54BEEB7A
        ECB9A566 5E43DF31 3C361B1A 9DC118D1 570D001F 3369934C
        33DC782E D003C8FA 6F04553D 01EBB34D D75721AB F8ADC9DB
        ED17889C BB9765D9 0A7C60F2 CEF007BB 0F2B26E1 4881FD44
        42E689D6 1CB2DD04 6EE30E3F FD20F9A4 5BBDF641 3D583A2D
        BF59924F D35C00F6 B632D194 C0388E22 D8437E55 8C552AE1
        95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
        B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4
```

```
MacKey is
                                                A649B1A5 7457DCB4
        15134A13 B4D9973D 13E48BA9 3B22A7A1 ED9F09EA BB493978


Mtag is
                         6713A8C4 B3567D00 CD75FF1A 6E053049
        F5455FD0 B2BAA262 9135CD12 B8D79A01 B2C56CCA D66C0AC0
        75D65028 48D20C2D DC65FB53 4DFD29F7 504CC145 1A17B67F


KeyData is
                                                A5E301CF 7FCF1D12
        37E26111 8CBED7AD E92EF2ED 856A6309 3182B539 40BE7572
        E914505F A51461C4 F4B889C0 8BFB0442 0C994ED1 05EB68B9
        8EAF6E42 41E84F8F 3A4C8BF8 A62B694F 05FC5338 65A7B6AB
        EEC2D8A2 25019C14 6B17A14E AB572BD0 B3A85D44 9099783D
        4F192877 B712A0BD 12B53459 A8342F13 4D5C5717 AA34ECC5




OnePassMQV(P-521)
-------------------------------------------------------------
dsU is
                      017D 1527DCC7 C046E4D3 04600ED0 D3A625F6
        AA46C475 14D92CB6 A6416C1B 8978B3E6 E9796830 6FFC49D0
        0371CCBD 4B796AA3 6547A6ED 3E78BBDF F2CFF34C E4C57FC9


QsU_x is
                      00D0 C2D9A667 F85A3C27 0C838535 04616791
        F3052858 3CF2D5CD D35D4E77 D440FE51 01DFC0E1 953983A9
        C1D7C330 7E6213FB CEB3D113 460D7B45 BBACAE5D 54B68166


QsU_y is
                      01C8 A85F0367 B3B1F4DE 8A74021E 08E13EA5
        65EF012E 647DD317 3B21DD6B B9987155 73063EBB 3152CAA7
        91ABD47F D31FB528 799413F8 DFF76E28 64E9870A 262ECACB


dsV is
                      00A0 752E306C ECD87AB0 E4830DA1 44F8038C
        E7B8C2B3 E5422ACF 9AAA6CCF 21818316 9A4CCA2A D577A64E
        6D86DCBF F5C1727A 11FD1CB8 E3A53842 B84005FD A9AC7F36
```

```
QsV_x is
                    0128 C16B23A4 259C9FE4 257C1DA4 3C7735C4
        3337929E 0FD86CC2 A778975B 67184CC2 825F6E66 7876D404
        BBF03E04 1F8FAD2F CCC036CD 5448B64E 9BD7DF6F 537659BB


QsV_y is
                    0108 089A6431 FED52344 DD5859A0 E5432D16
        9BEE36F5 3F857AED 08A69FE3 07B1C94B 8ABDCF65 0C4D1297
        29D69FB7 7D1CC1CD 651C676B 309CE018 C9771EAB 9CA5A754


deU is
                    0113 F82DA825 735E3D97 276683B2 B74277BA
        D27335EA 71664AF2 430CC4F3 3459B966 9EE78B3F FB9B8683
        015D344D CBFEF6FB 9AF4C6C4 70BE2545 16CD3C1A 1FB47362


QeU_x is
                    01EB B34DD757 21ABF8AD C9DBED17 889CBB97
        65D90A7C 60F2CEF0 07BB0F2B 26E14881 FD4442E6 89D61CB2
        DD046EE3 0E3FFD20 F9A45BBD F6413D58 3A2DBF59 924FD35C


QeU_y is
                    00F6 B632D194 C0388E22 D8437E55 8C552AE1
        95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
        B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4




------------------------------------------------------------
no Key Confirmation
Z is
                    0142 29035D7F 7F1F6331 0B786136 5902C246
        ED7ABF91 F13A5D38 12588D67 AECF74D5 4DA191F8 A2938F53
        71772870 853C9228 85875BBC 8A5103AB ED01D10C E2B9F381


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536
```

```
DerivedKeyMaterial is
                                                3F753BE6 F4789EF7
        118B0A21 9B14B011 484791A0 1A0D32D3 0585F595 55B61063
        68FBF512 FE36483B 8EBF4945 BBE2D2D9 278D9BBE CCF18F26
        A0CE02A6 8DBB57E7 749E0542 F225E2AC 1A1BC554 742B1810
        6A3E4508 C757F13C B86D2DD9 845357C2 AB460A67 A2652DBC
        FB409A2A C0E8F29A 41BAAB96 773216B6 A0127A56 69FA8577


KeyData is
                                                3F753BE6 F4789EF7
        118B0A21 9B14B011 484791A0 1A0D32D3 0585F595 55B61063
        68FBF512 FE36483B 8EBF4945 BBE2D2D9 278D9BBE CCF18F26
        A0CE02A6 8DBB57E7 749E0542 F225E2AC 1A1BC554 742B1810
        6A3E4508 C757F13C B86D2DD9 845357C2 AB460A67 A2652DBC
        FB409A2A C0E8F29A 41BAAB96 773216B6 A0127A56 69FA8577




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                    0020 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
        9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D


Z is
                    0142 29035D7F 7F1F6331 0B786136 5902C246
        ED7ABF91 F13A5D38 12588D67 AECF74D5 4DA191F8 A2938F53
        71772870 853C9228 85875BBC 8A5103AB ED01D10C E2B9F381


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                          3F753BE6 F4789EF7 118B0A21 9B14B011
        484791A0 1A0D32D3 0585F595 55B61063 68FBF512 FE36483B
        8EBF4945 BBE2D2D9 278D9BBE CCF18F26 A0CE02A6 8DBB57E7
        749E0542 F225E2AC 1A1BC554 742B1810 6A3E4508 C757F13C
        B86D2DD9 845357C2 AB460A67 A2652DBC FB409A2A C0E8F29A
        41BAAB96 773216B6 A0127A56 69FA8577 5274B1D9 603A560E
        F94E8641 43A458AD 6BDF9083 7BB2ACD6 FDF48123 2BF66CC4
```

```
MacData is
            4B43 5F315F55 414C4943 45424F42 425901EB B34DD757
         21ABF8AD C9DBED17 889CBB97 65D90A7C 60F2CEF0 07BB0F2B
         26E14881 FD4442E6 89D61CB2 DD046EE3 0E3FFD20 F9A45BBD
         F6413D58 3A2DBF59 924FD35C 00F6B632 D194C038 8E22D843
         7E558C55 2AE195AD FD153F92 D7490835 1B2F8C4E DA94EDB0
         916D1B53 C020B5EE CAED1A5F C38A233E 4830587B B2EE3489
         B3B42A5A 86A40020 905F7F3A 0298275E 33482000 1D90F0B2
         F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
         9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D


MacKey is
                                                 3F753BE6 F4789EF7
         118B0A21 9B14B011 484791A0 1A0D32D3 0585F595 55B61063


Mtag is
                           6E07FA4C E93B7E89 24BBBD0D C61AE9E0
         B2907CCB B2DF2469 6C80BA0C 7E0229D0 F5929E85 FE1EF024
         65FA9DEF 8FA1D8CC 3AEB08B9 C9206E8D 6DE6AE99 B81C1757


KeyData is
                                                 68FBF512 FE36483B
         8EBF4945 BBE2D2D9 278D9BBE CCF18F26 A0CE02A6 8DBB57E7
         749E0542 F225E2AC 1A1BC554 742B1810 6A3E4508 C757F13C
         B86D2DD9 845357C2 AB460A67 A2652DBC FB409A2A C0E8F29A
         41BAAB96 773216B6 A0127A56 69FA8577 5274B1D9 603A560E
         F94E8641 43A458AD 6BDF9083 7BB2ACD6 FDF48123 2BF66CC4




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
                      0020 905F7F3A 0298275E 33482000 1D90F0B2
         F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
         9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D


Z is
                      0142 29035D7F 7F1F6331 0B786136 5902C246
```

```
        ED7ABF91 F13A5D38 12588D67 AECF74D5 4DA191F8 A2938F53
        71772870 853C9228 85875BBC 8A5103AB ED01D10C E2B9F381


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         3F753BE6 F4789EF7 118B0A21 9B14B011
        484791A0 1A0D32D3 0585F595 55B61063 68FBF512 FE36483B
        8EBF4945 BBE2D2D9 278D9BBE CCF18F26 A0CE02A6 8DBB57E7
        749E0542 F225E2AC 1A1BC554 742B1810 6A3E4508 C757F13C
        B86D2DD9 845357C2 AB460A67 A2652DBC FB409A2A C0E8F29A
        41BAAB96 773216B6 A0127A56 69FA8577 5274B1D9 603A560E
        F94E8641 43A458AD 6BDF9083 7BB2ACD6 FDF48123 2BF66CC4


MacData is
                                                    4B435F31
        5F56424F 42425941 4C494345 01EBB34D D75721AB F8ADC9DB
        ED17889C BB9765D9 0A7C60F2 CEF007BB 0F2B26E1 4881FD44
        42E689D6 1CB2DD04 6EE30E3F FD20F9A4 5BBDF641 3D583A2D
        BF59924F D35C00F6 B632D194 C0388E22 D8437E55 8C552AE1
        95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
        B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4


MacKey is
                                            3F753BE6 F4789EF7
        118B0A21 9B14B011 484791A0 1A0D32D3 0585F595 55B61063


Mtag is
                         0B6E0BC7 95CFEF22 0326AA13 6DEB0779
        CBA2A842 721CCD74 80B1F98F 7ADA003C 8111D8BF E0AA540C
        E4F1A392 A00F8685 4B96BD55 9C7DB7E3 E0D0D776 4F399775


KeyData is
                                            68FBF512 FE36483B
        8EBF4945 BBE2D2D9 278D9BBE CCF18F26 A0CE02A6 8DBB57E7
        749E0542 F225E2AC 1A1BC554 742B1810 6A3E4508 C757F13C
        B86D2DD9 845357C2 AB460A67 A2652DBC FB409A2A C0E8F29A
        41BAAB96 773216B6 A0127A56 69FA8577 5274B1D9 603A560E
        F94E8641 43A458AD 6BDF9083 7BB2ACD6 FDF48123 2BF66CC4
```

```
------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
                    0020 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
        9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D


Z is
                    0142 29035D7F 7F1F6331 0B786136 5902C246
        ED7ABF91 F13A5D38 12588D67 AECF74D5 4DA191F8 A2938F53
        71772870 853C9228 85875BBC 8A5103AB ED01D10C E2B9F381


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         3F753BE6 F4789EF7 118B0A21 9B14B011
        484791A0 1A0D32D3 0585F595 55B61063 68FBF512 FE36483B
        8EBF4945 BBE2D2D9 278D9BBE CCF18F26 A0CE02A6 8DBB57E7
        749E0542 F225E2AC 1A1BC554 742B1810 6A3E4508 C757F13C
        B86D2DD9 845357C2 AB460A67 A2652DBC FB409A2A C0E8F29A
        41BAAB96 773216B6 A0127A56 69FA8577 5274B1D9 603A560E
        F94E8641 43A458AD 6BDF9083 7BB2ACD6 FDF48123 2BF66CC4


U2V
----------------
MacData is
            4B43 5F325F55 414C4943 45424F42 425901EB B34DD757
        21ABF8AD C9DBED17 889CBB97 65D90A7C 60F2CEF0 07BB0F2B
        26E14881 FD4442E6 89D61CB2 DD046EE3 0E3FFD20 F9A45BBD
        F6413D58 3A2DBF59 924FD35C 00F6B632 D194C038 8E22D843
        7E558C55 2AE195AD FD153F92 D7490835 1B2F8C4E DA94EDB0
        916D1B53 C020B5EE CAED1A5F C38A233E 4830587B B2EE3489
        B3B42A5A 86A40020 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
        9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D
```

```
MacKey is
                                                3F753BE6 F4789EF7
        118B0A21 9B14B011 484791A0 1A0D32D3 0585F595 55B61063


Mtag is
                         7F400BD7 E1E64884 309B256E 2CA57375
        EEFB825E EB117058 0BB4FADC 2DC23484 ADEAAE61 79BC6292
        BDC84C22 8ABC28BF 99B1064D 4842C6CD D20F1244 19A03AC1


V2U
----------------
MacData is
            4B43 5F325F56 424F4242 59414C49 43450020 905F7F3A
        0298275E 33482000 1D90F0B2 F19737D1 F8452AC5 54BEEB7A
        ECB9A566 5E43DF31 3C361B1A 9DC118D1 570D001F 3369934C
        33DC782E D003C8FA 6F04553D 01EBB34D D75721AB F8ADC9DB
        ED17889C BB9765D9 0A7C60F2 CEF007BB 0F2B26E1 4881FD44
        42E689D6 1CB2DD04 6EE30E3F FD20F9A4 5BBDF641 3D583A2D
        BF59924F D35C00F6 B632D194 C0388E22 D8437E55 8C552AE1
        95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
        B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4


MacKey is
                                                3F753BE6 F4789EF7
        118B0A21 9B14B011 484791A0 1A0D32D3 0585F595 55B61063


Mtag is
                         63017ABC 7778F87D 061C9247 B2E58A18
        9102C27B 100B00D3 FBD132D4 677F26B9 58A6C5E7 4C050F82
        7C5E5A72 A7F7AFF2 E9745287 EF1D8DB9 C199C9BA 180FB0D5


KeyData is
                                                68FBF512 FE36483B
        8EBF4945 BBE2D2D9 278D9BBE CCF18F26 A0CE02A6 8DBB57E7
        749E0542 F225E2AC 1A1BC554 742B1810 6A3E4508 C757F13C
        B86D2DD9 845357C2 AB460A67 A2652DBC FB409A2A C0E8F29A
        41BAAB96 773216B6 A0127A56 69FA8577 5274B1D9 603A560E
        F94E8641 43A458AD 6BDF9083 7BB2ACD6 FDF48123 2BF66CC4
```

OnePassDiffieHellmanCDH(P-521)
---
dsV is
00A0 752E306C ECD87AB0 E4830DA1 44F8038C
E7B8C2B3 E5422ACF 9AAA6CCF 21818316 9A4CCA2A D577A64E
6D86DCBF F5C1727A 11FD1CB8 E3A53842 B84005FD A9AC7F36

QsV_x is
0128 C16B23A4 259C9FE4 257C1DA4 3C7735C4
3337929E 0FD86CC2 A778975B 67184CC2 825F6E66 7876D404
BBF03E04 1F8FAD2F CCC036CD 5448B64E 9BD7DF6F 537659BB

QsV_y is
0108 089A6431 FED52344 DD5859A0 E5432D16
9BEE36F5 3F857AED 08A69FE3 07B1C94B 8ABDCF65 0C4D1297
29D69FB7 7D1CC1CD 651C676B 309CE018 C9771EAB 9CA5A754

deU is
0113 F82DA825 735E3D97 276683B2 B74277BA
D27335EA 71664AF2 430CC4F3 3459B966 9EE78B3F FB9B8683
015D344D CBFEF6FB 9AF4C6C4 70BE2545 16CD3C1A 1FB47362

QeU_x is
01EB B34DD757 21ABF8AD C9DBED17 889CBB97
65D90A7C 60F2CEF0 07BB0F2B 26E14881 FD4442E6 89D61CB2
DD046EE3 0E3FFD20 F9A45BBD F6413D58 3A2DBF59 924FD35C

QeU_y is
00F6 B632D194 C0388E22 D8437E55 8C552AE1
95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4

---
no Key Confirmation
Z is
0104 F83D9416 E8BB0FEB CBAC67FE CA3F23A1
54E9ECE9 CE152A38 1308754A E68B575A 67D0BA3E 7FAB218C

74C58BEF DB2E494D 510158A2 5EF077C1 D1C89E58 5F1C44F7

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
C0F84A40 108F717A
B9B7270C B8483BFA 4B2769E3 420C7259 C5E9FF93 F806C623
878B2215 E5784481 5B7AA0B6 BF36B690 BDCAE103 F1A24DB3
C6C3B58F 10B3A545 CD718E8B 358E1EE2 F9707D5F 54C8693A
E313F1C2 0737706B DDC7813C F0AB701F 27DC1382 8DB5FAC8
28455FF9 4AD3E1ED BA60FA73 5112F751 755ACF29 2AAF0D52

KeyData is
C0F84A40 108F717A
B9B7270C B8483BFA 4B2769E3 420C7259 C5E9FF93 F806C623
878B2215 E5784481 5B7AA0B6 BF36B690 BDCAE103 F1A24DB3
C6C3B58F 10B3A545 CD718E8B 358E1EE2 F9707D5F 54C8693A
E313F1C2 0737706B DDC7813C F0AB701F 27DC1382 8DB5FAC8
28455FF9 4AD3E1ED BA60FA73 5112F751 755ACF29 2AAF0D52

Scheme Responder, Key Confirmation Provider: V to U
Z is
0104 F83D9416 E8BB0FEB CBAC67FE CA3F23A1
54E9ECE9 CE152A38 1308754A E68B575A 67D0BA3E 7FAB218C
74C58BEF DB2E494D 510158A2 5EF077C1 D1C89E58 5F1C44F7

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
C0F84A40 108F717A B9B7270C B8483BFA
4B2769E3 420C7259 C5E9FF93 F806C623 878B2215 E5784481
5B7AA0B6 BF36B690 BDCAE103 F1A24DB3 C6C3B58F 10B3A545
CD718E8B 358E1EE2 F9707D5F 54C8693A E313F1C2 0737706B
DDC7813C F0AB701F 27DC1382 8DB5FAC8 28455FF9 4AD3E1ED
BA60FA73 5112F751 755ACF29 2AAF0D52 2CD329F4 B4266D87

```
        217A098B B81B8A26 9DD3A410 78668E31 74C0E4B9 D0A1F216


MacData is
                                                          4B435F31
        5F56424F 42425941 4C494345 01EBB34D D75721AB F8ADC9DB
        ED17889C BB9765D9 0A7C60F2 CEF007BB 0F2B26E1 4881FD44
        42E689D6 1CB2DD04 6EE30E3F FD20F9A4 5BBDF641 3D583A2D
        BF59924F D35C00F6 B632D194 C0388E22 D8437E55 8C552AE1
        95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
        B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4


MacKey is
                                               C0F84A40 108F717A
        B9B7270C B8483BFA 4B2769E3 420C7259 C5E9FF93 F806C623


Mtag is
                          9A8B208D 0DBB8215 E8E3F003 3F626C5C
        28B9953D 20E6B824 1DBB13EB 31557C04 9ABFCC60 D9990DEB
        ABF29DBF D3780D8A D3786313 CA4609CE 4A37F833 086A3CF8


KeyData is
                                               878B2215 E5784481
        5B7AA0B6 BF36B690 BDCAE103 F1A24DB3 C6C3B58F 10B3A545
        CD718E8B 358E1EE2 F9707D5F 54C8693A E313F1C2 0737706B
        DDC7813C F0AB701F 27DC1382 8DB5FAC8 28455FF9 4AD3E1ED
        BA60FA73 5112F751 755ACF29 2AAF0D52 2CD329F4 B4266D87
        217A098B B81B8A26 9DD3A410 78668E31 74C0E4B9 D0A1F216




StaticUnifiedCDH(P-521)
-----------------------------------------------------------
dsU is
                     017D 1527DCC7 C046E4D3 04600ED0 D3A625F6
        AA46C475 14D92CB6 A6416C1B 8978B3E6 E9796830 6FFC49D0
        0371CCBD 4B796AA3 6547A6ED 3E78BBDF F2CFF34C E4C57FC9


QsU_x is
                     00D0 C2D9A667 F85A3C27 0C838535 04616791
        F3052858 3CF2D5CD D35D4E77 D440FE51 01DFC0E1 953983A9
```

```
        C1D7C330 7E6213FB CEB3D113 460D7B45 BBACAE5D 54B68166


QsU_y is
                    01C8 A85F0367 B3B1F4DE 8A74021E 08E13EA5
        65EF012E 647DD317 3B21DD6B B9987155 73063EBB 3152CAA7
        91ABD47F D31FB528 799413F8 DFF76E28 64E9870A 262ECACB


dsV is
                    00A0 752E306C ECD87AB0 E4830DA1 44F8038C
        E7B8C2B3 E5422ACF 9AAA6CCF 21818316 9A4CCA2A D577A64E
        6D86DCBF F5C1727A 11FD1CB8 E3A53842 B84005FD A9AC7F36


QsV_x is
                    0128 C16B23A4 259C9FE4 257C1DA4 3C7735C4
        3337929E 0FD86CC2 A778975B 67184CC2 825F6E66 7876D404
        BBF03E04 1F8FAD2F CCC036CD 5448B64E 9BD7DF6F 537659BB


QsV_y is
                    0108 089A6431 FED52344 DD5859A0 E5432D16
        9BEE36F5 3F857AED 08A69FE3 07B1C94B 8ABDCF65 0C4D1297
        29D69FB7 7D1CC1CD 651C676B 309CE018 C9771EAB 9CA5A754




------------------------------------------------------------
no Key Confirmation
NonceU is
                    0020 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
        9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D


Z is
                    0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


OtherInfo is
                12345678 9ABCDEF0 414C4943 45313233 09020020
        905F7F3A 0298275E 33482000 1D90F0B2 F19737D1 F8452AC5
```

54BEEB7A ECB9A566 5E43DF31 3C361B1A 9DC118D1 570D001F
3369934C 33DC782E D003C8FA 6F04553D 424F4242 59343536

DerivedKeyMaterial is

502F5BC5 F0934777
2ECCB85C D867B79D 223D080A AD76E94B F9A6405D 5E9EBE81
5AC18328 52CC526F 21E850C7 113402B5 B1B8CF67 78CE4F43
AE3741BC 55B709D6 0B7DDE38 D0AC5501 2024E212 C714FB0C
39C122DA F6136D8E A2CC4359 F597A606 E99566A4 3E515AD7
23008707 1409F0FD 6A7D0F2E 230791B9 90F6A12C 5DD5E9F3

KeyData is

502F5BC5 F0934777
2ECCB85C D867B79D 223D080A AD76E94B F9A6405D 5E9EBE81
5AC18328 52CC526F 21E850C7 113402B5 B1B8CF67 78CE4F43
AE3741BC 55B709D6 0B7DDE38 D0AC5501 2024E212 C714FB0C
39C122DA F6136D8E A2CC4359 F597A606 E99566A4 3E515AD7
23008707 1409F0FD 6A7D0F2E 230791B9 90F6A12C 5DD5E9F3

Scheme Initiator, Key Confirmation Provider: U to V
NonceU is

0020 905F7F3A 0298275E 33482000 1D90F0B2
F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D

NonceV is

002A 26EAF7F8 44D4C41E 622F4AA9 17AB5F06
5A452352 1700C41A 5234B396 83680BCE F996099C 67FE5B46
6C1BAD07 A6C7F0F1 BBBFA3E2 A538CEA8 5A3C5936 3BEC365D

Z is

0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4

OtherInfo is

12345678 9ABCDEF0 414C4943 45313233 09020020

```
        905F7F3A 0298275E 33482000 1D90F0B2 F19737D1 F8452AC5
        54BEEB7A ECB9A566 5E43DF31 3C361B1A 9DC118D1 570D001F
        3369934C 33DC782E D003C8FA 6F04553D 424F4242 59343536


DerivedKeyMaterial is
                         502F5BC5 F0934777 2ECCB85C D867B79D
        223D080A AD76E94B F9A6405D 5E9EBE81 5AC18328 52CC526F
        21E850C7 113402B5 B1B8CF67 78CE4F43 AE3741BC 55B709D6
        0B7DDE38 D0AC5501 2024E212 C714FB0C 39C122DA F6136D8E
        A2CC4359 F597A606 E99566A4 3E515AD7 23008707 1409F0FD
        6A7D0F2E 230791B9 90F6A12C 5DD5E9F3 4E9CE662 1224DBED
        54E0005C 2AC6F95A 30808D45 EE4C8AB6 FFC5FBAC BE07CDEB


MacData is
                                                    4B435F31
        5F55414C 49434542 4F424259 0020905F 7F3A0298 275E3348
        20001D90 F0B2F197 37D1F845 2AC554BE EB7AECB9 A5665E43
        DF313C36 1B1A9DC1 18D1570D 001F3369 934C33DC 782ED003
        C8FA6F04 553D002A 26EAF7F8 44D4C41E 622F4AA9 17AB5F06
        5A452352 1700C41A 5234B396 83680BCE F996099C 67FE5B46
        6C1BAD07 A6C7F0F1 BBBFA3E2 A538CEA8 5A3C5936 3BEC365D


MacKey is
                                           502F5BC5 F0934777
        2ECCB85C D867B79D 223D080A AD76E94B F9A6405D 5E9EBE81


Mtag is
                         A12E81CA 6179767B 1F9849C2 F0200354
        6C404E9E B7FCB6AD 2A567DB7 B19BBCF5 A4838DDD C791CD8B
        28D70C36 FBADD63E B1D35A75 E31194FD 6BE45449 D1452D49


KeyData is
                                           5AC18328 52CC526F
        21E850C7 113402B5 B1B8CF67 78CE4F43 AE3741BC 55B709D6
        0B7DDE38 D0AC5501 2024E212 C714FB0C 39C122DA F6136D8E
        A2CC4359 F597A606 E99566A4 3E515AD7 23008707 1409F0FD
        6A7D0F2E 230791B9 90F6A12C 5DD5E9F3 4E9CE662 1224DBED
        54E0005C 2AC6F95A 30808D45 EE4C8AB6 FFC5FBAC BE07CDEB
```

```
------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceV is
                    002A 26EAF7F8 44D4C41E 622F4AA9 17AB5F06
        5A452352 1700C41A 5234B396 83680BCE F996099C 67FE5B46
        6C1BAD07 A6C7F0F1 BBBFA3E2 A538CEA8 5A3C5936 3BEC365D


NonceU is
                    0020 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
        9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D


Z is
                    0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


OtherInfo is
                12345678 9ABCDEF0 414C4943 45313233 09020020
        905F7F3A 0298275E 33482000 1D90F0B2 F19737D1 F8452AC5
        54BEEB7A ECB9A566 5E43DF31 3C361B1A 9DC118D1 570D001F
        3369934C 33DC782E D003C8FA 6F04553D 424F4242 59343536


DerivedKeyMaterial is
                        502F5BC5 F0934777 2ECCB85C D867B79D
        223D080A AD76E94B F9A6405D 5E9EBE81 5AC18328 52CC526F
        21E850C7 113402B5 B1B8CF67 78CE4F43 AE3741BC 55B709D6
        0B7DDE38 D0AC5501 2024E212 C714FB0C 39C122DA F6136D8E
        A2CC4359 F597A606 E99566A4 3E515AD7 23008707 1409F0FD
        6A7D0F2E 230791B9 90F6A12C 5DD5E9F3 4E9CE662 1224DBED
        54E0005C 2AC6F95A 30808D45 EE4C8AB6 FFC5FBAC BE07CDEB


MacData is
                                    4B43 5F315F56 424F4242
        59414C49 43450020 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
        9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D


MacKey is
```

```
                                                502F5BC5 F0934777
        2ECCB85C D867B79D 223D080A AD76E94B F9A6405D 5E9EBE81


Mtag is
                            332E2BED 457524D1 B542DF81 38F54D95
        AEC9D484 C579996F 871BAEFC B503972F ED5A34B9 99D4FD28
        63A018CA CC05BB83 3F1E0521 43904468 80AA12E5 59C3E57A


KeyData is
                                                5AC18328 52CC526F
        21E850C7 113402B5 B1B8CF67 78CE4F43 AE3741BC 55B709D6
        0B7DDE38 D0AC5501 2024E212 C714FB0C 39C122DA F6136D8E
        A2CC4359 F597A606 E99566A4 3E515AD7 23008707 1409F0FD
        6A7D0F2E 230791B9 90F6A12C 5DD5E9F3 4E9CE662 1224DBED
        54E0005C 2AC6F95A 30808D45 EE4C8AB6 FFC5FBAC BE07CDEB




------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
NonceU is
                       0020 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
        9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D


NonceV is
                       002A 26EAF7F8 44D4C41E 622F4AA9 17AB5F06
        5A452352 1700C41A 5234B396 83680BCE F996099C 67FE5B46
        6C1BAD07 A6C7F0F1 BBBFA3E2 A538CEA8 5A3C5936 3BEC365D


Z is
                       0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


OtherInfo is
                    12345678 9ABCDEF0 414C4943 45313233 09020020
        905F7F3A 0298275E 33482000 1D90F0B2 F19737D1 F8452AC5
        54BEEB7A ECB9A566 5E43DF31 3C361B1A 9DC118D1 570D001F
```

```
        3369934C 33DC782E D003C8FA 6F04553D 424F4242 59343536


DerivedKeyMaterial is
                         502F5BC5 F0934777 2ECCB85C D867B79D
        223D080A AD76E94B F9A6405D 5E9EBE81 5AC18328 52CC526F
        21E850C7 113402B5 B1B8CF67 78CE4F43 AE3741BC 55B709D6
        0B7DDE38 D0AC5501 2024E212 C714FB0C 39C122DA F6136D8E
        A2CC4359 F597A606 E99566A4 3E515AD7 23008707 1409F0FD
        6A7D0F2E 230791B9 90F6A12C 5DD5E9F3 4E9CE662 1224DBED
        54E0005C 2AC6F95A 30808D45 EE4C8AB6 FFC5FBAC BE07CDEB


U2V
----------------
MacData is
                                                    4B435F32
        5F55414C 49434542 4F424259 0020905F 7F3A0298 275E3348
        20001D90 F0B2F197 37D1F845 2AC554BE EB7AECB9 A5665E43
        DF313C36 1B1A9DC1 18D1570D 001F3369 934C33DC 782ED003
        C8FA6F04 553D002A 26EAF7F8 44D4C41E 622F4AA9 17AB5F06
        5A452352 1700C41A 5234B396 83680BCE F996099C 67FE5B46
        6C1BAD07 A6C7F0F1 BBBFA3E2 A538CEA8 5A3C5936 3BEC365D


MacKey is
                                            502F5BC5 F0934777
        2ECCB85C D867B79D 223D080A AD76E94B F9A6405D 5E9EBE81


Mtag is
                         858013F9 A125A145 CDE0839A 16109570
        01E5CE24 137679E1 73DBAF5C 2853C810 81C746BD AEF5AC60
        F7CE18F0 D532AE82 9BAD7FCB B64D92DE 40C13B3B B8F21769


V2U
----------------
MacData is
                                                    4B435F32
        5F56424F 42425941 4C494345 002A26EA F7F844D4 C41E622F
        4AA917AB 5F065A45 23521700 C41A5234 B3968368 0BCEF996
        099C67FE 5B466C1B AD07A6C7 F0F1BBBF A3E2A538 CEA85A3C
        59363BEC 365D0020 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
        9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D
```

MacKey is

```
                                            502F5BC5 F0934777
        2ECCB85C D867B79D 223D080A AD76E94B F9A6405D 5E9EBE81
```

Mtag is

```
                         0FBB421D 3538D824 DBA92CFB EE51D96D
        9420F397 5AA02313 BE8F5D6F 72696C09 486A377A FF68F8E8
        1609DCEC A874B2C2 07547A42 58956874 6B1F8E1E E70EC90C
```

KeyData is

```
                                            5AC18328 52CC526F
        21E850C7 113402B5 B1B8CF67 78CE4F43 AE3741BC 55B709D6
        0B7DDE38 D0AC5501 2024E212 C714FB0C 39C122DA F6136D8E
        A2CC4359 F597A606 E99566A4 3E515AD7 23008707 1409F0FD
        6A7D0F2E 230791B9 90F6A12C 5DD5E9F3 4E9CE662 1224DBED
        54E0005C 2AC6F95A 30808D45 EE4C8AB6 FFC5FBAC BE07CDEB
```

FullUnifiedCDH(K-163)
---
dsU is
02 AACC2BFB 50ACC96E 5C6B2BC9 9A48A742 99057E34

QsU_x is
00 02CEAEEA 30E62969 06CE4FAC DCAAB352 76B10D2B

QsU_y is
05 28B0F4C4 EF361FEC 8E1FF67F 520A56CC 73F727D7

dsV is
01 B81A3747 A5BA47F9 D8D71918 B1330D1E 6A3FD3AE

QsV_x is
04 55C84BF0 5F3D08A9 740BED76 DB6AFFA0 FF49E447

QsV_y is
02 34493742 ED1C40E8 435DBA3D 5AD4A5B5 5175E1FA

deU is
00 EC6AF27A 975F3138 2207F9B2 B74A6423 4B57D008

QeU_x is
01 A7DFE2C9 3F5A2A78 0384A9AD DB63AE5F 73AFDD36

QeU_y is
04 C6C8219B 1AE4A46F 076E9329 C956A94F 62B54B51

deV is
02 CE70BED4 0833693F DD78886D AA20495F 005563D4

QeV_x is
04 F1B128CF 49F1A423 7114C912 910DA06A AACC7A86

QeV_y is
00 E8EFF57A FD8D6283 167ECBD2 595D5305 C5B717E7

---

no Key Confirmation
Zs is
03 AE195657 3786A33C B976C42A 6792D611 CE5AEBCC

Ze is
04 4EA63C13 9BC92E98 F366D541 238573A5 73D51713

Z is
044E A63C139B C92E98F3 66D54123 8573A573
D5171303 AE195657 3786A33C B976C42A 6792D611 CE5AEBCC

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
6B7F3FC0 396315F9 B15664D7 2BB93D3F
B99D462A 8378ACDE 575D8FC8 DF27AE51 9188F6BE 894BBB86

KeyData is
6B7F3FC0 396315F9 B15664D7 2BB93D3F
B99D462A 8378ACDE 575D8FC8 DF27AE51 9188F6BE 894BBB86

Scheme Initiator, Key Confirmation Provider: U to V
Zs is
03 AE195657 3786A33C B976C42A 6792D611 CE5AEBCC

Ze is

```
              04 4EA63C13 9BC92E98 F366D541 238573A5 73D51713


Z is
                     044E A63C139B C92E98F3 66D54123 8573A573
         D5171303 AE195657 3786A33C B976C42A 6792D611 CE5AEBCC


OtherInfo is
         12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            6B7F
         3FC03963 15F9B156 64D72BB9 3D3FB99D 462A8378 ACDE575D
         8FC8DF27 AE519188 F6BE894B BB8687FB E8C8768D 57C697F8


MacData is
                                                          4B435F31
         5F55414C 49434542 4F424259 01A7DFE2 C93F5A2A 780384A9
         ADDB63AE 5F73AFDD 3604C6C8 219B1AE4 A46F076E 9329C956
         A94F62B5 4B5104F1 B128CF49 F1A42371 14C91291 0DA06AAA
         CC7A8600 E8EFF57A FD8D6283 167ECBD2 595D5305 C5B717E7


MacKey is
                                       6B7F 3FC03963 15F9B156


Mtag is
                 DDA7FBD0 DD37B603 3D382651 1115578B 6EC55646


KeyData is
                          64D72BB9 3D3FB99D 462A8378 ACDE575D
         8FC8DF27 AE519188 F6BE894B BB8687FB E8C8768D 57C697F8




-------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Zs is
              03 AE195657 3786A33C B976C42A 6792D611 CE5AEBCC
```

```
Ze is
              04 4EA63C13 9BC92E98 F366D541 238573A5 73D51713


Z is
                     044E A63C139B C92E98F3 66D54123 8573A573
         D5171303 AE195657 3786A33C B976C42A 6792D611 CE5AEBCC


OtherInfo is
         12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            6B7F
         3FC03963 15F9B156 64D72BB9 3D3FB99D 462A8378 ACDE575D
         8FC8DF27 AE519188 F6BE894B BB8687FB E8C8768D 57C697F8


MacData is
                                                          4B435F31
         5F56424F 42425941 4C494345 04F1B128 CF49F1A4 237114C9
         12910DA0 6AAACC7A 8600E8EF F57AFD8D 6283167E CBD2595D
         5305C5B7 17E701A7 DFE2C93F 5A2A7803 84A9ADDB 63AE5F73
         AFDD3604 C6C8219B 1AE4A46F 076E9329 C956A94F 62B54B51


MacKey is
                                       6B7F 3FC03963 15F9B156


Mtag is
                  F57D2B14 B7D81804 0F4F66FD 79FE05DC 5AC36D7F


KeyData is
                           64D72BB9 3D3FB99D 462A8378 ACDE575D
         8FC8DF27 AE519188 F6BE894B BB8687FB E8C8768D 57C697F8




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
Zs is
```

```
             03 AE195657 3786A33C B976C42A 6792D611 CE5AEBCC


Ze is
             04 4EA63C13 9BC92E98 F366D541 238573A5 73D51713


Z is
                   044E A63C139B C92E98F3 66D54123 8573A573
        D5171303 AE195657 3786A33C B976C42A 6792D611 CE5AEBCC


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                          6B7F
        3FC03963 15F9B156 64D72BB9 3D3FB99D 462A8378 ACDE575D
        8FC8DF27 AE519188 F6BE894B BB8687FB E8C8768D 57C697F8


U2V
----------------
MacData is
                                                    4B435F32
        5F55414C 49434542 4F424259 01A7DFE2 C93F5A2A 780384A9
        ADDB63AE 5F73AFDD 3604C6C8 219B1AE4 A46F076E 9329C956
        A94F62B5 4B5104F1 B128CF49 F1A42371 14C91291 0DA06AAA
        CC7A8600 E8EFF57A FD8D6283 167ECBD2 595D5305 C5B717E7


MacKey is
                                     6B7F 3FC03963 15F9B156


Mtag is
                4EBD99C9 9E9D8F0C DAFFD861 92B10038 E09442F5


V2U
----------------
MacData is
                                                    4B435F32
        5F56424F 42425941 4C494345 04F1B128 CF49F1A4 237114C9
        12910DA0 6AAACC7A 8600E8EF F57AFD8D 6283167E CBD2595D
```

```
        5305C5B7 17E701A7 DFE2C93F 5A2A7803 84A9ADDB 63AE5F73
        AFDD3604 C6C8219B 1AE4A46F 076E9329 C956A94F 62B54B51


MacKey is
                                        6B7F 3FC03963 15F9B156


Mtag is
                3E69FBB9 13F75F1F 90CB5A56 1587551F 914AE6CB


KeyData is
                         64D72BB9 3D3FB99D 462A8378 ACDE575D
        8FC8DF27 AE519188 F6BE894B BB8687FB E8C8768D 57C697F8




FullMQV(K-163)
-------------------------------------------------------------
dsU is
             02 AACC2BFB 50ACC96E 5C6B2BC9 9A48A742 99057E34


QsU_x is
             00 02CEAEEA 30E62969 06CE4FAC DCAAB352 76B10D2B


QsU_y is
             05 28B0F4C4 EF361FEC 8E1FF67F 520A56CC 73F727D7


dsV is
             01 B81A3747 A5BA47F9 D8D71918 B1330D1E 6A3FD3AE


QsV_x is
             04 55C84BF0 5F3D08A9 740BED76 DB6AFFA0 FF49E447


QsV_y is
             02 34493742 ED1C40E8 435DBA3D 5AD4A5B5 5175E1FA


deU is
```

```
              00 EC6AF27A 975F3138 2207F9B2 B74A6423 4B57D008


QeU_x is
              01 A7DFE2C9 3F5A2A78 0384A9AD DB63AE5F 73AFDD36


QeU_y is
              04 C6C8219B 1AE4A46F 076E9329 C956A94F 62B54B51


deV is
              02 CE70BED4 0833693F DD78886D AA20495F 005563D4


QeV_x is
              04 F1B128CF 49F1A423 7114C912 910DA06A AACC7A86


QeV_y is
              00 E8EFF57A FD8D6283 167ECBD2 595D5305 C5B717E7




-------------------------------------------------------------
no Key Confirmation
Z is
              01 44AE4574 1A93DAB5 C0310118 C6B3ECD3 BA1E532B


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         4294C735 C143D5D1 D6690A04 323DDFAC
        5BF55558 02B41E4C DCA2A35D C7953948 35AFADDD 14D728BD


KeyData is
                         4294C735 C143D5D1 D6690A04 323DDFAC
        5BF55558 02B41E4C DCA2A35D C7953948 35AFADDD 14D728BD
```

```
-----------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Z is
              01 44AE4574 1A93DAB5 C0310118 C6B3ECD3 BA1E532B


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                          4294
        C735C143 D5D1D669 0A04323D DFAC5BF5 555802B4 1E4CDCA2
        A35DC795 394835AF ADDD14D7 28BD3052 357C0E7E 5F5E3149


MacData is
                                                        4B435F31
        5F55414C 49434542 4F424259 01A7DFE2 C93F5A2A 780384A9
        ADDB63AE 5F73AFDD 3604C6C8 219B1AE4 A46F076E 9329C956
        A94F62B5 4B5104F1 B128CF49 F1A42371 14C91291 0DA06AAA
        CC7A8600 E8EFF57A FD8D6283 167ECBD2 595D5305 C5B717E7


MacKey is
                                     4294 C735C143 D5D1D669


Mtag is
                63650724 CBC0E1D6 3C130332 6973106E FFBD09BA


KeyData is
                         0A04323D DFAC5BF5 555802B4 1E4CDCA2
        A35DC795 394835AF ADDD14D7 28BD3052 357C0E7E 5F5E3149




-----------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
              01 44AE4574 1A93DAB5 C0310118 C6B3ECD3 BA1E532B
```

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                              4294
        C735C143 D5D1D669 0A04323D DFAC5BF5 555802B4 1E4CDCA2
        A35DC795 394835AF ADDD14D7 28BD3052 357C0E7E 5F5E3149


MacData is
                                                          4B435F31
        5F56424F 42425941 4C494345 04F1B128 CF49F1A4 237114C9
        12910DA0 6AAACC7A 8600E8EF F57AFD8D 6283167E CBD2595D
        5305C5B7 17E701A7 DFE2C93F 5A2A7803 84A9ADDB 63AE5F73
        AFDD3604 C6C8219B 1AE4A46F 076E9329 C956A94F 62B54B51


MacKey is
                                      4294 C735C143 D5D1D669


Mtag is
                E25E1E8C 35A66152 7825C4E3 9C51A221 FD43D85F


KeyData is
                          0A04323D DFAC5BF5 555802B4 1E4CDCA2
        A35DC795 394835AF ADDD14D7 28BD3052 357C0E7E 5F5E3149




------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
Z is
             01 44AE4574 1A93DAB5 C0310118 C6B3ECD3 BA1E532B


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                              4294
```

```
        C735C143 D5D1D669 0A04323D DFAC5BF5 555802B4 1E4CDCA2
        A35DC795 394835AF ADDD14D7 28BD3052 357C0E7E 5F5E3149


U2V
----------------
MacData is
                                                    4B435F32
        5F55414C 49434542 4F424259 01A7DFE2 C93F5A2A 780384A9
        ADDB63AE 5F73AFDD 3604C6C8 219B1AE4 A46F076E 9329C956
        A94F62B5 4B5104F1 B128CF49 F1A42371 14C91291 0DA06AAA
        CC7A8600 E8EFF57A FD8D6283 167ECBD2 595D5305 C5B717E7


MacKey is
                                    4294 C735C143 D5D1D669


Mtag is
                2358FB31 BBE7BCC7 6C3EC72B BAC0276E 60099DE0


V2U
----------------
MacData is
                                                    4B435F32
        5F56424F 42425941 4C494345 04F1B128 CF49F1A4 237114C9
        12910DA0 6AAACC7A 8600E8EF F57AFD8D 6283167E CBD2595D
        5305C5B7 17E701A7 DFE2C93F 5A2A7803 84A9ADDB 63AE5F73
        AFDD3604 C6C8219B 1AE4A46F 076E9329 C956A94F 62B54B51


MacKey is
                                    4294 C735C143 D5D1D669


Mtag is
                46F3A4A8 462455FF FFBFB8A3 BF7542CD A121FD22


KeyData is
                         0A04323D DFAC5BF5 555802B4 1E4CDCA2
        A35DC795 394835AF ADDD14D7 28BD3052 357C0E7E 5F5E3149
```

```
EphemeralUnifiedCDH(K-163)
------------------------------------------------------------
deU is
              00 EC6AF27A 975F3138 2207F9B2 B74A6423 4B57D008


QeU_x is
              01 A7DFE2C9 3F5A2A78 0384A9AD DB63AE5F 73AFDD36


QeU_y is
              04 C6C8219B 1AE4A46F 076E9329 C956A94F 62B54B51


deV is
              02 CE70BED4 0833693F DD78886D AA20495F 005563D4


QeV_x is
              04 F1B128CF 49F1A423 7114C912 910DA06A AACC7A86


QeV_y is
              00 E8EFF57A FD8D6283 167ECBD2 595D5305 C5B717E7




------------------------------------------------------------
no Key Confirmation
Z is
              04 4EA63C13 9BC92E98 F366D541 238573A5 73D51713


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                           F2C4A323 0979B225 19948DFF 5FEA5A21
        947A3483 7A59D432 D503E56B C56BB0E4 3B1792DC 3A2D9068


KeyData is
                           F2C4A323 0979B225 19948DFF 5FEA5A21
```

947A3483 7A59D432 D503E56B C56BB0E4 3B1792DC 3A2D9068

OnePassUnifiedCDH(K-163)
---
dsU is
02 AACC2BFB 50ACC96E 5C6B2BC9 9A48A742 99057E34

QsU_x is
00 02CEAEEA 30E62969 06CE4FAC DCAAB352 76B10D2B

QsU_y is
05 28B0F4C4 EF361FEC 8E1FF67F 520A56CC 73F727D7

dsV is
01 B81A3747 A5BA47F9 D8D71918 B1330D1E 6A3FD3AE

QsV_x is
04 55C84BF0 5F3D08A9 740BED76 DB6AFFA0 FF49E447

QsV_y is
02 34493742 ED1C40E8 435DBA3D 5AD4A5B5 5175E1FA

deU is
00 EC6AF27A 975F3138 2207F9B2 B74A6423 4B57D008

QeU_x is
01 A7DFE2C9 3F5A2A78 0384A9AD DB63AE5F 73AFDD36

QeU_y is
04 C6C8219B 1AE4A46F 076E9329 C956A94F 62B54B51

---

no Key Confirmation
Zs is
03 AE195657 3786A33C B976C42A 6792D611 CE5AEBCC

Ze is
06 86151068 A669A2AE 47F1E906 E525D180 52F4A791

Z is
0686 151068A6 69A2AE47 F1E906E5 25D18052
F4A79103 AE195657 3786A33C B976C42A 6792D611 CE5AEBCC

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
EC63D366 FC07C485 00C4844C 42D2A5EA
7AFEF4AA 39431296 2C0233B1 DEA918AF C24B223C D4543953

KeyData is
EC63D366 FC07C485 00C4844C 42D2A5EA
7AFEF4AA 39431296 2C0233B1 DEA918AF C24B223C D4543953

Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
00 04887A73 FC382E5F 1349DF8A A4729188 03ACEB82

Zs is
03 AE195657 3786A33C B976C42A 6792D611 CE5AEBCC

Ze is
06 86151068 A669A2AE 47F1E906 E525D180 52F4A791

Z is
0686 151068A6 69A2AE47 F1E906E5 25D18052

F4A79103 AE195657 3786A33C B976C42A 6792D611 CE5AEBCC

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
EC63
D366FC07 C48500C4 844C42D2 A5EA7AFE F4AA3943 12962C02
33B1DEA9 18AFC24B 223CD454 39536F4B 7FCF323C DFB0E506

MacData is
4B435F 315F5541
4C494345 424F4242 5901A7DF E2C93F5A 2A780384 A9ADDB63
AE5F73AF DD3604C6 C8219B1A E4A46F07 6E9329C9 56A94F62
B54B5100 04887A73 FC382E5F 1349DF8A A4729188 03ACEB82

MacKey is
EC63 D366FC07 C48500C4

Mtag is
FAA73D8A E19B7026 7EE1C8CD 1723F33D FFEF26AA

KeyData is
844C42D2 A5EA7AFE F4AA3943 12962C02
33B1DEA9 18AFC24B 223CD454 39536F4B 7FCF323C DFB0E506

Scheme Responder, Key Confirmation Provider: V to U
NonceU is
00 04887A73 FC382E5F 1349DF8A A4729188 03ACEB82

Zs is
03 AE195657 3786A33C B976C42A 6792D611 CE5AEBCC

Ze is

```
              06 86151068 A669A2AE 47F1E906 E525D180 52F4A791


Z is
                     0686 151068A6 69A2AE47 F1E906E5 25D18052
         F4A79103 AE195657 3786A33C B976C42A 6792D611 CE5AEBCC


OtherInfo is
         12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            EC63
         D366FC07 C48500C4 844C42D2 A5EA7AFE F4AA3943 12962C02
         33B1DEA9 18AFC24B 223CD454 39536F4B 7FCF323C DFB0E506


MacData is
                                       4B43 5F315F56 424F4242
         59414C49 434501A7 DFE2C93F 5A2A7803 84A9ADDB 63AE5F73
         AFDD3604 C6C8219B 1AE4A46F 076E9329 C956A94F 62B54B51


MacKey is
                                       EC63 D366FC07 C48500C4


Mtag is
                 4C64F76E C0E437B7 AEF9E019 1F1BD409 EDF78B7D


KeyData is
                           844C42D2 A5EA7AFE F4AA3943 12962C02
         33B1DEA9 18AFC24B 223CD454 39536F4B 7FCF323C DFB0E506




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
              00 04887A73 FC382E5F 1349DF8A A4729188 03ACEB82


Zs is
```

```
              03 AE195657 3786A33C B976C42A 6792D611 CE5AEBCC


Ze is
              06 86151068 A669A2AE 47F1E906 E525D180 52F4A791


Z is
                     0686 151068A6 69A2AE47 F1E906E5 25D18052
         F4A79103 AE195657 3786A33C B976C42A 6792D611 CE5AEBCC


OtherInfo is
         12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                             EC63
         D366FC07 C48500C4 844C42D2 A5EA7AFE F4AA3943 12962C02
         33B1DEA9 18AFC24B 223CD454 39536F4B 7FCF323C DFB0E506


U2V
----------------
MacData is
                                               4B435F 325F5541
         4C494345 424F4242 5901A7DF E2C93F5A 2A780384 A9ADDB63
         AE5F73AF DD3604C6 C8219B1A E4A46F07 6E9329C9 56A94F62
         B54B5100 04887A73 FC382E5F 1349DF8A A4729188 03ACEB82


MacKey is
                                        EC63 D366FC07 C48500C4


Mtag is
                  A93E23A9 BD1A2602 F398CB87 339871C5 8F895130


V2U
----------------
MacData is
                                               4B435F 325F5642
         4F424259 414C4943 45000488 7A73FC38 2E5F1349 DF8AA472
         918803AC EB8201A7 DFE2C93F 5A2A7803 84A9ADDB 63AE5F73
         AFDD3604 C6C8219B 1AE4A46F 076E9329 C956A94F 62B54B51
```

MacKey is
                                        EC63 D366FC07 C48500C4

Mtag is
                C9DDFDA0 9FA8BCDF E5FC26EB 611CCD85 0549174B

KeyData is
                          844C42D2 A5EA7AFE F4AA3943 12962C02
        33B1DEA9 18AFC24B 223CD454 39536F4B 7FCF323C DFB0E506

OnePassMQV(K-163)
----
dsU is
              02 AACC2BFB 50ACC96E 5C6B2BC9 9A48A742 99057E34

QsU_x is
              00 02CEAEEA 30E62969 06CE4FAC DCAAB352 76B10D2B

QsU_y is
              05 28B0F4C4 EF361FEC 8E1FF67F 520A56CC 73F727D7

dsV is
              01 B81A3747 A5BA47F9 D8D71918 B1330D1E 6A3FD3AE

QsV_x is
              04 55C84BF0 5F3D08A9 740BED76 DB6AFFA0 FF49E447

QsV_y is
              02 34493742 ED1C40E8 435DBA3D 5AD4A5B5 5175E1FA

deU is
              00 EC6AF27A 975F3138 2207F9B2 B74A6423 4B57D008

QeU_x is
              01 A7DFE2C9 3F5A2A78 0384A9AD DB63AE5F 73AFDD36

QeU_y is
              04 C6C8219B 1AE4A46F 076E9329 C956A94F 62B54B51

---
no Key Confirmation
Z is
              00 A86474A4 E2780AE2 29952672 00A37257 4DD55BDE

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                           02CCFAB0 10114859 34A59D39 DBD69114
        B4EDF829 3DB88C94 0DEF001D A32E1FFD BC5E7F43 E78004D9

KeyData is
                           02CCFAB0 10114859 34A59D39 DBD69114
        B4EDF829 3DB88C94 0DEF001D A32E1FFD BC5E7F43 E78004D9

Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
              00 04887A73 FC382E5F 1349DF8A A4729188 03ACEB82

Z is
              00 A86474A4 E2780AE2 29952672 00A37257 4DD55BDE

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

```
DerivedKeyMaterial is
                                                              02CC
        FAB01011 485934A5 9D39DBD6 9114B4ED F8293DB8 8C940DEF
        001DA32E 1FFDBC5E 7F43E780 04D9C705 194EF3E7 C5F1391E


MacData is
                                                 4B435F 315F5541
        4C494345 424F4242 5901A7DF E2C93F5A 2A780384 A9ADDB63
        AE5F73AF DD3604C6 C8219B1A E4A46F07 6E9329C9 56A94F62
        B54B5100 04887A73 FC382E5F 1349DF8A A4729188 03ACEB82


MacKey is
                                       02CC FAB01011 485934A5


Mtag is
                7DF0AA22 E6B3A1E7 DBA19809 C30204D9 D540EF60


KeyData is
                          9D39DBD6 9114B4ED F8293DB8 8C940DEF
        001DA32E 1FFDBC5E 7F43E780 04D9C705 194EF3E7 C5F1391E




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
              00 04887A73 FC382E5F 1349DF8A A4729188 03ACEB82


Z is
              00 A86474A4 E2780AE2 29952672 00A37257 4DD55BDE


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                              02CC
        FAB01011 485934A5 9D39DBD6 9114B4ED F8293DB8 8C940DEF
```

```
        001DA32E 1FFDBC5E 7F43E780 04D9C705 194EF3E7 C5F1391E


MacData is
                                        4B43 5F315F56 424F4242
        59414C49 434501A7 DFE2C93F 5A2A7803 84A9ADDB 63AE5F73
        AFDD3604 C6C8219B 1AE4A46F 076E9329 C956A94F 62B54B51


MacKey is
                                        02CC FAB01011 485934A5


Mtag is
                7FFAFB1F 060BB2FA 0F2CE340 C156BB49 57C62495


KeyData is
                          9D39DBD6 9114B4ED F8293DB8 8C940DEF
        001DA32E 1FFDBC5E 7F43E780 04D9C705 194EF3E7 C5F1391E




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
              00 04887A73 FC382E5F 1349DF8A A4729188 03ACEB82


Z is
              00 A86474A4 E2780AE2 29952672 00A37257 4DD55BDE


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            02CC
        FAB01011 485934A5 9D39DBD6 9114B4ED F8293DB8 8C940DEF
        001DA32E 1FFDBC5E 7F43E780 04D9C705 194EF3E7 C5F1391E


U2V
----------------
```

```
MacData is
                                                  4B435F 325F5541
        4C494345 424F4242 5901A7DF E2C93F5A 2A780384 A9ADDB63
        AE5F73AF DD3604C6 C8219B1A E4A46F07 6E9329C9 56A94F62
        B54B5100 04887A73 FC382E5F 1349DF8A A4729188 03ACEB82


MacKey is
                                       02CC FAB01011 485934A5


Mtag is
                C568D154 07100B64 72405127 EA9791D9 7A802A77


V2U
----------------
MacData is
                                                  4B435F 325F5642
        4F424259 414C4943 45000488 7A73FC38 2E5F1349 DF8AA472
        918803AC EB8201A7 DFE2C93F 5A2A7803 84A9ADDB 63AE5F73
        AFDD3604 C6C8219B 1AE4A46F 076E9329 C956A94F 62B54B51


MacKey is
                                       02CC FAB01011 485934A5


Mtag is
                69D52BAE 37A3AF76 38E0A60A C828D5BC 3955B2E3


KeyData is
                          9D39DBD6 9114B4ED F8293DB8 8C940DEF
        001DA32E 1FFDBC5E 7F43E780 04D9C705 194EF3E7 C5F1391E




OnePassDiffieHellmanCDH(K-163)
------------------------------------------------------------
dsV is
              01 B81A3747 A5BA47F9 D8D71918 B1330D1E 6A3FD3AE


QsV_x is
```

```
              04 55C84BF0 5F3D08A9 740BED76 DB6AFFA0 FF49E447

QsV_y is
              02 34493742 ED1C40E8 435DBA3D 5AD4A5B5 5175E1FA

deU is
              00 EC6AF27A 975F3138 2207F9B2 B74A6423 4B57D008

QeU_x is
              01 A7DFE2C9 3F5A2A78 0384A9AD DB63AE5F 73AFDD36

QeU_y is
              04 C6C8219B 1AE4A46F 076E9329 C956A94F 62B54B51




------------------------------------------------------------
no Key Confirmation
Z is
              06 86151068 A669A2AE 47F1E906 E525D180 52F4A791

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                         EF77404B 8B7D64BC 2BFDE60B A9A23821
        78890589 D5015F27 17C7231F 212F7759 32DF5B2D 19EAAE37

KeyData is
                         EF77404B 8B7D64BC 2BFDE60B A9A23821
        78890589 D5015F27 17C7231F 212F7759 32DF5B2D 19EAAE37




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
```

```
              06 86151068 A669A2AE 47F1E906 E525D180 52F4A791


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            EF77
        404B8B7D 64BC2BFD E60BA9A2 38217889 0589D501 5F2717C7
        231F212F 775932DF 5B2D19EA AE375C16 FB39491A DEC655B1


MacData is
                                       4B43 5F315F56 424F4242
        59414C49 434501A7 DFE2C93F 5A2A7803 84A9ADDB 63AE5F73
        AFDD3604 C6C8219B 1AE4A46F 076E9329 C956A94F 62B54B51


MacKey is
                                       EF77 404B8B7D 64BC2BFD


Mtag is
                 A8369139 44DDFC9E BE7A3996 BC1393CF 05B1D550


KeyData is
                           E60BA9A2 38217889 0589D501 5F2717C7
        231F212F 775932DF 5B2D19EA AE375C16 FB39491A DEC655B1




StaticUnifiedCDH(K-163)
-------------------------------------------------------------
dsU is
              02 6FAC5107 DDB6EDD6 06E8034E 48C8F879 E478F6BE


QsU_x is
              06 87EC97B8 41058E50 93116E30 22A386DD 75C3C9FB


QsU_y is
              02 2AD69EE6 DE1BA795 8F74CA8B 7C10422F 9984D476
```

```
dsV is
              00 6302F726 39832BA1 F0DF0ED6 D356BAC9 1BE1A2CC


QsV_x is
              04 0D66F3CC D7B5E5D0 50A7FFDC D0D681B1 9F820DAB


QsV_y is
              04 F83E2FB2 1D45CAEB 340A6D0B 71BB2B49 8F72EFAD




------------------------------------------------------------
no Key Confirmation
NonceU is
              00 04887A73 FC382E5F 1349DF8A A4729188 03ACEB82


Z is
              03 885F119E C8850E2F 52CC10E2 BCA0E9B8 3B966C4D


OtherInfo is
             1234 56789ABC DEF0414C 49434531 3233A300 04887A73
        FC382E5F 1349DF8A A4729188 03ACEB82 424F4242 59343536


DerivedKeyMaterial is
                           F46BF73D E9F4EF0B E5FE573C 6110C803
        2E367A9A 4443D04E 99C29A18 0FC29128 65A435C5 431F12F0


KeyData is
                           F46BF73D E9F4EF0B E5FE573C 6110C803
        2E367A9A 4443D04E 99C29A18 0FC29128 65A435C5 431F12F0




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceU is
```

```
              00 04887A73 FC382E5F 1349DF8A A4729188 03ACEB82


NonceV is
              01 B780DDBC 14856EE8 A1C110F6 FE204E37 CA50F7FD


Z is
              03 885F119E C8850E2F 52CC10E2 BCA0E9B8 3B966C4D


OtherInfo is
             1234 56789ABC DEF0414C 49434531 3233A300 04887A73
         FC382E5F 1349DF8A A4729188 03ACEB82 424F4242 59343536


DerivedKeyMaterial is
                                                              F46B
         F73DE9F4 EF0BE5FE 573C6110 C8032E36 7A9A4443 D04E99C2
         9A180FC2 912865A4 35C5431F 12F0027E 58CAA750 8DED114F


MacData is
                                       4B43 5F315F55 414C4943
         45424F42 42590004 887A73FC 382E5F13 49DF8AA4 72918803
         ACEB8201 B780DDBC 14856EE8 A1C110F6 FE204E37 CA50F7FD


MacKey is
                                       F46B F73DE9F4 EF0BE5FE


Mtag is
                 8DAE8597 A6486293 267A4003 08D1D21B 80C705C0


KeyData is
                          573C6110 C8032E36 7A9A4443 D04E99C2
         9A180FC2 912865A4 35C5431F 12F0027E 58CAA750 8DED114F




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceV is
```

```
              01 B780DDBC 14856EE8 A1C110F6 FE204E37 CA50F7FD


NonceU is
              00 04887A73 FC382E5F 1349DF8A A4729188 03ACEB82


Z is
              03 885F119E C8850E2F 52CC10E2 BCA0E9B8 3B966C4D


OtherInfo is
             1234 56789ABC DEF0414C 49434531 3233A300 04887A73
         FC382E5F 1349DF8A A4729188 03ACEB82 424F4242 59343536


DerivedKeyMaterial is
                                                             F46B
         F73DE9F4 EF0BE5FE 573C6110 C8032E36 7A9A4443 D04E99C2
         9A180FC2 912865A4 35C5431F 12F0027E 58CAA750 8DED114F


MacData is
                                4B 435F315F 56424F42 4259414C
         49434500 04887A73 FC382E5F 1349DF8A A4729188 03ACEB82


MacKey is
                                      F46B F73DE9F4 EF0BE5FE


Mtag is
                  E129952C 8CAB8484 B983E2DB 1A6759BE 2B4136B6


KeyData is
                           573C6110 C8032E36 7A9A4443 D04E99C2
         9A180FC2 912865A4 35C5431F 12F0027E 58CAA750 8DED114F




------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
NonceU is
```

```
              00 04887A73 FC382E5F 1349DF8A A4729188 03ACEB82


NonceV is
              01 B780DDBC 14856EE8 A1C110F6 FE204E37 CA50F7FD


Z is
              03 885F119E C8850E2F 52CC10E2 BCA0E9B8 3B966C4D


OtherInfo is
             1234 56789ABC DEF0414C 49434531 3233A300 04887A73
         FC382E5F 1349DF8A A4729188 03ACEB82 424F4242 59343536


DerivedKeyMaterial is
                                                             F46B
         F73DE9F4 EF0BE5FE 573C6110 C8032E36 7A9A4443 D04E99C2
         9A180FC2 912865A4 35C5431F 12F0027E 58CAA750 8DED114F


U2V
----------------
MacData is
                                       4B43 5F325F55 414C4943
         45424F42 42590004 887A73FC 382E5F13 49DF8AA4 72918803
         ACEB8201 B780DDBC 14856EE8 A1C110F6 FE204E37 CA50F7FD


MacKey is
                                       F46B F73DE9F4 EF0BE5FE


Mtag is
                  CFF1971F 0DC44184 EBDAC948 B2372E4A D3EC6F25


V2U
----------------
MacData is
                                       4B43 5F325F56 424F4242
         59414C49 434501B7 80DDBC14 856EE8A1 C110F6FE 204E37CA
         50F7FD00 04887A73 FC382E5F 1349DF8A A4729188 03ACEB82
```

MacKey is

F46B F73DE9F4 EF0BE5FE

Mtag is

593DE077 25E71ACA D9C35F0A 66AA22D1 40AB9E08

KeyData is

573C6110 C8032E36 7A9A4443 D04E99C2
9A180FC2 912865A4 35C5431F 12F0027E 58CAA750 8DED114F

FullUnifiedCDH(B-163)
---
dsU is
00 C54ACE26 2B8D2E7B 0ACC550A FF87FCF9 F9E537DD

QsU_x is
05 34BBB6C6 36238F1A C4DA4639 FB05B204 1186758E

QsU_y is
01 90D98DB4 8441CD1D EA2B333E 125FF7C8 2B7503D8

dsV is
03 16E8B99F 7D4502D9 CCCC27BD 1A25FD18 8FEB8BCB

QsV_x is
03 94FBFB66 7CC9D274 BE99600A C9F881D0 ADF985EB

QsV_y is
03 92FC2898 87AF4F94 14D5C9A6 A9A55428 3648A06A

deU is
00 4F6ABD7C 8FA28B99 255C92D1 4E7769C7 39415BE8

QeU_x is
06 CFB81985 3EE01586 3F234EA2 03F33432 356E9383

QeU_y is
01 7C87F656 5D9421A2 B0688D8D A6331BA0 052F76FB

deV is
01 491D6B51 D46FEF34 CB06B0FF 6CA0C054 BDBF2E87

QeV_x is
01 461D1F37 D2627DFA BFA9A8C2 90535462 5B7238F1

QeV_y is
              05 ED7F5C1A 4F8D4DA1 02BAEC81 0154A13D 079256EF

---
no Key Confirmation
Zs is
              03 BD725B8B 50BE2DD6 99BD6796 0880CD40 9C159318

Ze is
              05 1B018D61 85905DAF D67BB7E0 5103F62B 6095E863

Z is
                     051B 018D6185 905DAFD6 7BB7E051 03F62B60
        95E86303 BD725B8B 50BE2DD6 99BD6796 0880CD40 9C159318

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                           77FF188E 523842F1 016E74C2 58FB27ED
        4E9CBC6F 3C9D5124 D491F8B0 A666FD7F 0319186B F4C5ECDE

KeyData is
                           77FF188E 523842F1 016E74C2 58FB27ED
        4E9CBC6F 3C9D5124 D491F8B0 A666FD7F 0319186B F4C5ECDE

Scheme Initiator, Key Confirmation Provider: U to V
Zs is
              03 BD725B8B 50BE2DD6 99BD6796 0880CD40 9C159318

Ze is

```
              05 1B018D61 85905DAF D67BB7E0 5103F62B 6095E863


Z is
                     051B 018D6185 905DAFD6 7BB7E051 03F62B60
         95E86303 BD725B8B 50BE2DD6 99BD6796 0880CD40 9C159318


OtherInfo is
         12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                             77FF
         188E5238 42F1016E 74C258FB 27ED4E9C BC6F3C9D 5124D491
         F8B0A666 FD7F0319 186BF4C5 ECDEFE42 1912B710 5A2196E6


MacData is
                                                           4B435F31
         5F55414C 49434542 4F424259 06CFB819 853EE015 863F234E
         A203F334 32356E93 83017C87 F6565D94 21A2B068 8D8DA633
         1BA0052F 76FB0146 1D1F37D2 627DFABF A9A8C290 5354625B
         7238F105 ED7F5C1A 4F8D4DA1 02BAEC81 0154A13D 079256EF


MacKey is
                                       77FF 188E5238 42F1016E


Mtag is
                 E84AAD4F DA1CE7F9 880E92C7 2C8E2E4C 3F5ED05E


KeyData is
                           74C258FB 27ED4E9C BC6F3C9D 5124D491
         F8B0A666 FD7F0319 186BF4C5 ECDEFE42 1912B710 5A2196E6




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Zs is
              03 BD725B8B 50BE2DD6 99BD6796 0880CD40 9C159318
```

Ze is
             05 1B018D61 85905DAF D67BB7E0 5103F62B 6095E863

Z is
                   051B 018D6185 905DAFD6 7BB7E051 03F62B60
        95E86303 BD725B8B 50BE2DD6 99BD6796 0880CD40 9C159318

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                                                          77FF
        188E5238 42F1016E 74C258FB 27ED4E9C BC6F3C9D 5124D491
        F8B0A666 FD7F0319 186BF4C5 ECDEFE42 1912B710 5A2196E6

MacData is
                                                    4B435F31
        5F56424F 42425941 4C494345 01461D1F 37D2627D FABFA9A8
        C2905354 625B7238 F105ED7F 5C1A4F8D 4DA102BA EC810154
        A13D0792 56EF06CF B819853E E015863F 234EA203 F3343235
        6E938301 7C87F656 5D9421A2 B0688D8D A6331BA0 052F76FB

MacKey is
                                     77FF 188E5238 42F1016E

Mtag is
                39C771D8 1C46C59C 8925B685 3A821690 CBE0A44E

KeyData is
                         74C258FB 27ED4E9C BC6F3C9D 5124D491
        F8B0A666 FD7F0319 186BF4C5 ECDEFE42 1912B710 5A2196E6

Scheme Initiator, Key Confirmation Bilateral
Zs is

```
              03 BD725B8B 50BE2DD6 99BD6796 0880CD40 9C159318


Ze is
              05 1B018D61 85905DAF D67BB7E0 5103F62B 6095E863


Z is
                    051B 018D6185 905DAFD6 7BB7E051 03F62B60
        95E86303 BD725B8B 50BE2DD6 99BD6796 0880CD40 9C159318


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                           77FF
        188E5238 42F1016E 74C258FB 27ED4E9C BC6F3C9D 5124D491
        F8B0A666 FD7F0319 186BF4C5 ECDEFE42 1912B710 5A2196E6


U2V
----------------
MacData is
                                                    4B435F32
        5F55414C 49434542 4F424259 06CFB819 853EE015 863F234E
        A203F334 32356E93 83017C87 F6565D94 21A2B068 8D8DA633
        1BA0052F 76FB0146 1D1F37D2 627DFABF A9A8C290 5354625B
        7238F105 ED7F5C1A 4F8D4DA1 02BAEC81 0154A13D 079256EF


MacKey is
                                     77FF 188E5238 42F1016E


Mtag is
                5124B090 A5D03EA7 DCB0BB39 4312E6D5 456FDB7F


V2U
----------------
MacData is
                                                    4B435F32
        5F56424F 42425941 4C494345 01461D1F 37D2627D FABFA9A8
        C2905354 625B7238 F105ED7F 5C1A4F8D 4DA102BA EC810154
```

```
        A13D0792 56EF06CF B819853E E015863F 234EA203 F3343235
        6E938301 7C87F656 5D9421A2 B0688D8D A6331BA0 052F76FB


MacKey is
                                        77FF 188E5238 42F1016E


Mtag is
                A1C2B25B 4576352F E1246E8F B211AE90 8211A788


KeyData is
                          74C258FB 27ED4E9C BC6F3C9D 5124D491
        F8B0A666 FD7F0319 186BF4C5 ECDEFE42 1912B710 5A2196E6




FullMQV(B-163)
-------------------------------------------------------------
dsU is
             00 C54ACE26 2B8D2E7B 0ACC550A FF87FCF9 F9E537DD


QsU_x is
             05 34BBB6C6 36238F1A C4DA4639 FB05B204 1186758E


QsU_y is
             01 90D98DB4 8441CD1D EA2B333E 125FF7C8 2B7503D8


dsV is
             03 16E8B99F 7D4502D9 CCCC27BD 1A25FD18 8FEB8BCB


QsV_x is
             03 94FBFB66 7CC9D274 BE99600A C9F881D0 ADF985EB


QsV_y is
             03 92FC2898 87AF4F94 14D5C9A6 A9A55428 3648A06A


deU is
```

```
              00 4F6ABD7C 8FA28B99 255C92D1 4E7769C7 39415BE8


QeU_x is
              06 CFB81985 3EE01586 3F234EA2 03F33432 356E9383


QeU_y is
              01 7C87F656 5D9421A2 B0688D8D A6331BA0 052F76FB


deV is
              01 491D6B51 D46FEF34 CB06B0FF 6CA0C054 BDBF2E87


QeV_x is
              01 461D1F37 D2627DFA BFA9A8C2 90535462 5B7238F1


QeV_y is
              05 ED7F5C1A 4F8D4DA1 02BAEC81 0154A13D 079256EF




------------------------------------------------------------
no Key Confirmation
Z is
              01 63391641 501D2C09 60069A06 E42F0F9E 561357C0


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         C1C1B177 774266E4 64A90F68 2A764D88
        61FF0959 F52C1E68 7B3EACD9 2BE8A9F9 D275B5A0 374311E5


KeyData is
                         C1C1B177 774266E4 64A90F68 2A764D88
        61FF0959 F52C1E68 7B3EACD9 2BE8A9F9 D275B5A0 374311E5
```

```
-----------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Z is
              01 63391641 501D2C09 60069A06 E42F0F9E 561357C0


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                          C1C1
        B1777742 66E464A9 0F682A76 4D8861FF 0959F52C 1E687B3E
        ACD92BE8 A9F9D275 B5A03743 11E58EB2 BC5A29DD 23D5C99F


MacData is
                                                       4B435F31
        5F55414C 49434542 4F424259 06CFB819 853EE015 863F234E
        A203F334 32356E93 83017C87 F6565D94 21A2B068 8D8DA633
        1BA0052F 76FB0146 1D1F37D2 627DFABF A9A8C290 5354625B
        7238F105 ED7F5C1A 4F8D4DA1 02BAEC81 0154A13D 079256EF


MacKey is
                                     C1C1 B1777742 66E464A9


Mtag is
                 D3134A6B F3F34FCB EB566CCB 16B62500 07180A37


KeyData is
                          0F682A76 4D8861FF 0959F52C 1E687B3E
        ACD92BE8 A9F9D275 B5A03743 11E58EB2 BC5A29DD 23D5C99F




-----------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
              01 63391641 501D2C09 60069A06 E42F0F9E 561357C0
```

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            C1C1
        B1777742 66E464A9 0F682A76 4D8861FF 0959F52C 1E687B3E
        ACD92BE8 A9F9D275 B5A03743 11E58EB2 BC5A29DD 23D5C99F


MacData is
                                                          4B435F31
        5F56424F 42425941 4C494345 01461D1F 37D2627D FABFA9A8
        C2905354 625B7238 F105ED7F 5C1A4F8D 4DA102BA EC810154
        A13D0792 56EF06CF B819853E E015863F 234EA203 F3343235
        6E938301 7C87F656 5D9421A2 B0688D8D A6331BA0 052F76FB


MacKey is
                                       C1C1 B1777742 66E464A9


Mtag is
                5F3AEFF8 4B78747F 7F5CEEB3 FD07DA4D 6921AB9D


KeyData is
                          0F682A76 4D8861FF 0959F52C 1E687B3E
        ACD92BE8 A9F9D275 B5A03743 11E58EB2 BC5A29DD 23D5C99F




------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
Z is
              01 63391641 501D2C09 60069A06 E42F0F9E 561357C0


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            C1C1
```

```
        B1777742 66E464A9 0F682A76 4D8861FF 0959F52C 1E687B3E
        ACD92BE8 A9F9D275 B5A03743 11E58EB2 BC5A29DD 23D5C99F


U2V
----------------
MacData is
                                                    4B435F32
        5F55414C 49434542 4F424259 06CFB819 853EE015 863F234E
        A203F334 32356E93 83017C87 F6565D94 21A2B068 8D8DA633
        1BA0052F 76FB0146 1D1F37D2 627DFABF A9A8C290 5354625B
        7238F105 ED7F5C1A 4F8D4DA1 02BAEC81 0154A13D 079256EF


MacKey is
                                       C1C1 B1777742 66E464A9


Mtag is
                6C7C3C42 8E9A43B0 9236A9F3 0C081830 F128F920


V2U
----------------
MacData is
                                                    4B435F32
        5F56424F 42425941 4C494345 01461D1F 37D2627D FABFA9A8
        C2905354 625B7238 F105ED7F 5C1A4F8D 4DA102BA EC810154
        A13D0792 56EF06CF B819853E E015863F 234EA203 F3343235
        6E938301 7C87F656 5D9421A2 B0688D8D A6331BA0 052F76FB


MacKey is
                                       C1C1 B1777742 66E464A9


Mtag is
                68860E9F 31E1A402 992C8C8D 862127D8 856AD64E


KeyData is
                         0F682A76 4D8861FF 0959F52C 1E687B3E
        ACD92BE8 A9F9D275 B5A03743 11E58EB2 BC5A29DD 23D5C99F
```

EphemeralUnifiedCDH(B-163)

---

deU is
00 4F6ABD7C 8FA28B99 255C92D1 4E7769C7 39415BE8

QeU_x is
06 CFB81985 3EE01586 3F234EA2 03F33432 356E9383

QeU_y is
01 7C87F656 5D9421A2 B0688D8D A6331BA0 052F76FB

deV is
01 491D6B51 D46FEF34 CB06B0FF 6CA0C054 BDBF2E87

QeV_x is
01 461D1F37 D2627DFA BFA9A8C2 90535462 5B7238F1

QeV_y is
05 ED7F5C1A 4F8D4DA1 02BAEC81 0154A13D 079256EF

---

no Key Confirmation
Z is
05 1B018D61 85905DAF D67BB7E0 5103F62B 6095E863

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
AF501862 2DF486E4 AC6AB3FE 59E099BD
576DB467 708888C9 32B80705 01CF48B0 38C70291 DC8DF6D4

KeyData is
AF501862 2DF486E4 AC6AB3FE 59E099BD

576DB467 708888C9 32B80705 01CF48B0 38C70291 DC8DF6D4

OnePassUnifiedCDH(B-163)

---

dsU is

00 C54ACE26 2B8D2E7B 0ACC550A FF87FCF9 F9E537DD

QsU_x is

05 34BBB6C6 36238F1A C4DA4639 FB05B204 1186758E

QsU_y is

01 90D98DB4 8441CD1D EA2B333E 125FF7C8 2B7503D8

dsV is

03 16E8B99F 7D4502D9 CCCC27BD 1A25FD18 8FEB8BCB

QsV_x is

03 94FBFB66 7CC9D274 BE99600A C9F881D0 ADF985EB

QsV_y is

03 92FC2898 87AF4F94 14D5C9A6 A9A55428 3648A06A

deU is

00 4F6ABD7C 8FA28B99 255C92D1 4E7769C7 39415BE8

QeU_x is

06 CFB81985 3EE01586 3F234EA2 03F33432 356E9383

QeU_y is

01 7C87F656 5D9421A2 B0688D8D A6331BA0 052F76FB

---

no Key Confirmation
Zs is
              03 BD725B8B 50BE2DD6 99BD6796 0880CD40 9C159318

Ze is
              02 01483278 72A1ADFB B5461F0E 4852D039 F30E4B5D

Z is
                     0201 48327872 A1ADFBB5 461F0E48 52D039F3
        0E4B5D03 BD725B8B 50BE2DD6 99BD6796 0880CD40 9C159318

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                           E64C233F 863AEBA1 6AF2BBE3 B86F7F65
        721C5D81 4F00CBE7 E85E9E4F 70ABEA6F 5E39205C 5DA868BE

KeyData is
                           E64C233F 863AEBA1 6AF2BBE3 B86F7F65
        721C5D81 4F00CBE7 E85E9E4F 70ABEA6F 5E39205C 5DA868BE

Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
              00 774E07FF C5A3A7A8 85D16C4E F49F9380 91B49314

Zs is
              03 BD725B8B 50BE2DD6 99BD6796 0880CD40 9C159318

Ze is
              02 01483278 72A1ADFB B5461F0E 4852D039 F30E4B5D

Z is
                     0201 48327872 A1ADFBB5 461F0E48 52D039F3

```
        0E4B5D03 BD725B8B 50BE2DD6 99BD6796 0880CD40 9C159318


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            E64C
        233F863A EBA16AF2 BBE3B86F 7F65721C 5D814F00 CBE7E85E
        9E4F70AB EA6F5E39 205C5DA8 68BE6913 1B064DEC 0E7357DD


MacData is
                                              4B435F 315F5541
        4C494345 424F4242 5906CFB8 19853EE0 15863F23 4EA203F3
        3432356E 9383017C 87F6565D 9421A2B0 688D8DA6 331BA005
        2F76FB00 774E07FF C5A3A7A8 85D16C4E F49F9380 91B49314


MacKey is
                                     E64C 233F863A EBA16AF2


Mtag is
                209EE6A0 A961A7AC 517E9703 07F20F5B 1C18C593


KeyData is
                         BBE3B86F 7F65721C 5D814F00 CBE7E85E
        9E4F70AB EA6F5E39 205C5DA8 68BE6913 1B064DEC 0E7357DD




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
             00 774E07FF C5A3A7A8 85D16C4E F49F9380 91B49314


Zs is
             03 BD725B8B 50BE2DD6 99BD6796 0880CD40 9C159318


Ze is
```

```
              02 01483278 72A1ADFB B5461F0E 4852D039 F30E4B5D


Z is
                     0201 48327872 A1ADFBB5 461F0E48 52D039F3
         0E4B5D03 BD725B8B 50BE2DD6 99BD6796 0880CD40 9C159318


OtherInfo is
         12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            E64C
         233F863A EBA16AF2 BBE3B86F 7F65721C 5D814F00 CBE7E85E
         9E4F70AB EA6F5E39 205C5DA8 68BE6913 1B064DEC 0E7357DD


MacData is
                                       4B43 5F315F56 424F4242
         59414C49 434506CF B819853E E015863F 234EA203 F3343235
         6E938301 7C87F656 5D9421A2 B0688D8D A6331BA0 052F76FB


MacKey is
                                       E64C 233F863A EBA16AF2


Mtag is
                  3D3A0C42 B4E79AC0 2BD96CC2 C6426107 8E874C81


KeyData is
                            BBE3B86F 7F65721C 5D814F00 CBE7E85E
         9E4F70AB EA6F5E39 205C5DA8 68BE6913 1B064DEC 0E7357DD




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
              00 774E07FF C5A3A7A8 85D16C4E F49F9380 91B49314


Zs is
```

```
              03 BD725B8B 50BE2DD6 99BD6796 0880CD40 9C159318


Ze is
              02 01483278 72A1ADFB B5461F0E 4852D039 F30E4B5D


Z is
                    0201 48327872 A1ADFBB5 461F0E48 52D039F3
        0E4B5D03 BD725B8B 50BE2DD6 99BD6796 0880CD40 9C159318


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                           E64C
        233F863A EBA16AF2 BBE3B86F 7F65721C 5D814F00 CBE7E85E
        9E4F70AB EA6F5E39 205C5DA8 68BE6913 1B064DEC 0E7357DD


U2V
----------------
MacData is
                                                 4B435F 325F5541
        4C494345 424F4242 5906CFB8 19853EE0 15863F23 4EA203F3
        3432356E 9383017C 87F6565D 9421A2B0 688D8DA6 331BA005
        2F76FB00 774E07FF C5A3A7A8 85D16C4E F49F9380 91B49314


MacKey is
                                       E64C 233F863A EBA16AF2


Mtag is
                5B5C7ABD 9E76A379 5F3B7F2D EC42806A AD76BA30


V2U
----------------
MacData is
                                                 4B435F 325F5642
        4F424259 414C4943 4500774E 07FFC5A3 A7A885D1 6C4EF49F
        938091B4 931406CF B819853E E015863F 234EA203 F3343235
        6E938301 7C87F656 5D9421A2 B0688D8D A6331BA0 052F76FB
```

MacKey is
                                    E64C 233F863A EBA16AF2

Mtag is
                9E107E29 962D6132 86AB3980 13874C66 849D156F

KeyData is
                         BBE3B86F 7F65721C 5D814F00 CBE7E85E
        9E4F70AB EA6F5E39 205C5DA8 68BE6913 1B064DEC 0E7357DD

OnePassMQV(B-163)
----
dsU is
              00 C54ACE26 2B8D2E7B 0ACC550A FF87FCF9 F9E537DD

QsU_x is
              05 34BBB6C6 36238F1A C4DA4639 FB05B204 1186758E

QsU_y is
              01 90D98DB4 8441CD1D EA2B333E 125FF7C8 2B7503D8

dsV is
              03 16E8B99F 7D4502D9 CCCC27BD 1A25FD18 8FEB8BCB

QsV_x is
              03 94FBFB66 7CC9D274 BE99600A C9F881D0 ADF985EB

QsV_y is
              03 92FC2898 87AF4F94 14D5C9A6 A9A55428 3648A06A

deU is
              00 4F6ABD7C 8FA28B99 255C92D1 4E7769C7 39415BE8

QeU_x is
              06 CFB81985 3EE01586 3F234EA2 03F33432 356E9383

QeU_y is
              01 7C87F656 5D9421A2 B0688D8D A6331BA0 052F76FB

---
no Key Confirmation
Z is
              07 5079E94D EAE58A6A A96E8FF6 81AD7B0C B24C0D73

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                           BE54B16F 9713FEA3 B507E23A 88D6710B
        62F0C0B1 3349D545 E7D0D039 1E33AB19 ADF28EB7 8D2C687C

KeyData is
                           BE54B16F 9713FEA3 B507E23A 88D6710B
        62F0C0B1 3349D545 E7D0D039 1E33AB19 ADF28EB7 8D2C687C

Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
              00 774E07FF C5A3A7A8 85D16C4E F49F9380 91B49314

Z is
              07 5079E94D EAE58A6A A96E8FF6 81AD7B0C B24C0D73

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

```
DerivedKeyMaterial is
                                                              BE54
        B16F9713 FEA3B507 E23A88D6 710B62F0 C0B13349 D545E7D0
        D0391E33 AB19ADF2 8EB78D2C 687C5F43 F1CFBB4A 9CC372D1


MacData is
                                                 4B435F 315F5541
        4C494345 424F4242 5906CFB8 19853EE0 15863F23 4EA203F3
        3432356E 9383017C 87F6565D 9421A2B0 688D8DA6 331BA005
        2F76FB00 774E07FF C5A3A7A8 85D16C4E F49F9380 91B49314


MacKey is
                                       BE54 B16F9713 FEA3B507


Mtag is
                F29B4CDB 34CA4397 73685B37 E4FEB85C 159FA281


KeyData is
                          E23A88D6 710B62F0 C0B13349 D545E7D0
        D0391E33 AB19ADF2 8EB78D2C 687C5F43 F1CFBB4A 9CC372D1




-------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
              00 774E07FF C5A3A7A8 85D16C4E F49F9380 91B49314


Z is
              07 5079E94D EAE58A6A A96E8FF6 81AD7B0C B24C0D73


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                              BE54
        B16F9713 FEA3B507 E23A88D6 710B62F0 C0B13349 D545E7D0
```

```
        D0391E33 AB19ADF2 8EB78D2C 687C5F43 F1CFBB4A 9CC372D1


MacData is
                                        4B43 5F315F56 424F4242
        59414C49 434506CF B819853E E015863F 234EA203 F3343235
        6E938301 7C87F656 5D9421A2 B0688D8D A6331BA0 052F76FB


MacKey is
                                        BE54 B16F9713 FEA3B507


Mtag is
                A173BB82 2077FB0A 07DA5849 68969C15 0E2EBFE8


KeyData is
                         E23A88D6 710B62F0 C0B13349 D545E7D0
        D0391E33 AB19ADF2 8EB78D2C 687C5F43 F1CFBB4A 9CC372D1




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
              00 774E07FF C5A3A7A8 85D16C4E F49F9380 91B49314


Z is
              07 5079E94D EAE58A6A A96E8FF6 81AD7B0C B24C0D73


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            BE54
        B16F9713 FEA3B507 E23A88D6 710B62F0 C0B13349 D545E7D0
        D0391E33 AB19ADF2 8EB78D2C 687C5F43 F1CFBB4A 9CC372D1


U2V
----------------
```

```
MacData is
                                                  4B435F 325F5541
        4C494345 424F4242 5906CFB8 19853EE0 15863F23 4EA203F3
        3432356E 9383017C 87F6565D 9421A2B0 688D8DA6 331BA005
        2F76FB00 774E07FF C5A3A7A8 85D16C4E F49F9380 91B49314


MacKey is
                                       BE54 B16F9713 FEA3B507


Mtag is
                3C52F838 09E1AAE3 6F6B72E9 384E9C20 C68074BE


V2U
----------------
MacData is
                                                  4B435F 325F5642
        4F424259 414C4943 4500774E 07FFC5A3 A7A885D1 6C4EF49F
        938091B4 931406CF B819853E E015863F 234EA203 F3343235
        6E938301 7C87F656 5D9421A2 B0688D8D A6331BA0 052F76FB


MacKey is
                                       BE54 B16F9713 FEA3B507


Mtag is
                2D932536 59B48149 8A1A659F 8D9EB839 CD3E7639


KeyData is
                          E23A88D6 710B62F0 C0B13349 D545E7D0
        D0391E33 AB19ADF2 8EB78D2C 687C5F43 F1CFBB4A 9CC372D1




OnePassDiffieHellmanCDH(B-163)
------------------------------------------------------------
dsV is
              03 16E8B99F 7D4502D9 CCCC27BD 1A25FD18 8FEB8BCB


QsV_x is
```

```
              03 94FBFB66 7CC9D274 BE99600A C9F881D0 ADF985EB


QsV_y is
              03 92FC2898 87AF4F94 14D5C9A6 A9A55428 3648A06A


deU is
              00 4F6ABD7C 8FA28B99 255C92D1 4E7769C7 39415BE8


QeU_x is
              06 CFB81985 3EE01586 3F234EA2 03F33432 356E9383


QeU_y is
              01 7C87F656 5D9421A2 B0688D8D A6331BA0 052F76FB




------------------------------------------------------------
no Key Confirmation
Z is
              02 01483278 72A1ADFB B5461F0E 4852D039 F30E4B5D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         918E1FDA C9339DB9 186A693D 3D81BF75
        84B545EE F2E2E38E 04FE41BA 7BBD7682 AA1AB724 7EDDDBB5


KeyData is
                         918E1FDA C9339DB9 186A693D 3D81BF75
        84B545EE F2E2E38E 04FE41BA 7BBD7682 AA1AB724 7EDDDBB5




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
```

```
              02 01483278 72A1ADFB B5461F0E 4852D039 F30E4B5D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            918E
        1FDAC933 9DB9186A 693D3D81 BF7584B5 45EEF2E2 E38E04FE
        41BA7BBD 7682AA1A B7247EDD DBB522F9 E1E3177A 3E7A7BA5


MacData is
                                       4B43 5F315F56 424F4242
        59414C49 434506CF B819853E E015863F 234EA203 F3343235
        6E938301 7C87F656 5D9421A2 B0688D8D A6331BA0 052F76FB


MacKey is
                                       918E 1FDAC933 9DB9186A


Mtag is
                 72AEABB5 E9702EEB F270F562 C05B6F40 2B4AE109


KeyData is
                           693D3D81 BF7584B5 45EEF2E2 E38E04FE
        41BA7BBD 7682AA1A B7247EDD DBB522F9 E1E3177A 3E7A7BA5




StaticUnifiedCDH(B-163)
-----------------------------------------------------------
dsU is
              03 79ED4E86 A6106248 42446121 AD1EE034 C4709ED4


QsU_x is
              01 4D85611A 2F3202DE A67D0098 A01E0B6D A229FD29


QsU_y is
              01 BF07AF0F 09962CA7 B070507C D9672ADA 1E6E24AF
```

```
dsV is
              02 00A8A185 67406E86 C685CA40 16D86305 FAECB995


QsV_x is
              06 6576EA03 BFE215C1 75C1DDB9 F2523DDC F24CEB9A


QsV_y is
              04 F938ABF9 B8E35083 D2A1C6B8 906DBD96 11A9D643




------------------------------------------------------------
no Key Confirmation
NonceU is
              00 774E07FF C5A3A7A8 85D16C4E F49F9380 91B49314


Z is
              00 92361CC1 B0B2D3F7 F5A0B498 4D101CA7 0559AEB9


OtherInfo is
             1234 56789ABC DEF0414C 49434531 3233A300 774E07FF
        C5A3A7A8 85D16C4E F49F9380 91B49314 424F4242 59343536


DerivedKeyMaterial is
                           E3FF906C E89A8BD2 A61CC4ED 4E745B0A
        3DB5C6C2 9A8BF04B 19EC051F 3BA9A2F3 20F86B7D EFA2FDE8


KeyData is
                           E3FF906C E89A8BD2 A61CC4ED 4E745B0A
        3DB5C6C2 9A8BF04B 19EC051F 3BA9A2F3 20F86B7D EFA2FDE8




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceU is
```

```
              00 774E07FF C5A3A7A8 85D16C4E F49F9380 91B49314


NonceV is
              01 9AA2022D EAB805FA 2BA8044F BDAFBDDA 71D688D8


Z is
              00 92361CC1 B0B2D3F7 F5A0B498 4D101CA7 0559AEB9


OtherInfo is
             1234 56789ABC DEF0414C 49434531 3233A300 774E07FF
         C5A3A7A8 85D16C4E F49F9380 91B49314 424F4242 59343536


DerivedKeyMaterial is
                                                             E3FF
         906CE89A 8BD2A61C C4ED4E74 5B0A3DB5 C6C29A8B F04B19EC
         051F3BA9 A2F320F8 6B7DEFA2 FDE8C627 8E108B36 E595FC1A


MacData is
                                       4B43 5F315F55 414C4943
         45424F42 42590077 4E07FFC5 A3A7A885 D16C4EF4 9F938091
         B4931401 9AA2022D EAB805FA 2BA8044F BDAFBDDA 71D688D8


MacKey is
                                       E3FF 906CE89A 8BD2A61C


Mtag is
                  14F1E7B4 D18E7ECC 434F7C37 BB010BFD 939AC147


KeyData is
                           C4ED4E74 5B0A3DB5 C6C29A8B F04B19EC
         051F3BA9 A2F320F8 6B7DEFA2 FDE8C627 8E108B36 E595FC1A




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceV is
```

```
              01 9AA2022D EAB805FA 2BA8044F BDAFBDDA 71D688D8


NonceU is
              00 774E07FF C5A3A7A8 85D16C4E F49F9380 91B49314


Z is
              00 92361CC1 B0B2D3F7 F5A0B498 4D101CA7 0559AEB9


OtherInfo is
             1234 56789ABC DEF0414C 49434531 3233A300 774E07FF
         C5A3A7A8 85D16C4E F49F9380 91B49314 424F4242 59343536


DerivedKeyMaterial is
                                                             E3FF
         906CE89A 8BD2A61C C4ED4E74 5B0A3DB5 C6C29A8B F04B19EC
         051F3BA9 A2F320F8 6B7DEFA2 FDE8C627 8E108B36 E595FC1A


MacData is
                                4B 435F315F 56424F42 4259414C
         49434500 774E07FF C5A3A7A8 85D16C4E F49F9380 91B49314


MacKey is
                                       E3FF 906CE89A 8BD2A61C


Mtag is
                 DD66CE23 6F9173D5 BEBF1761 1D4B4B96 AA3373E1


KeyData is
                           C4ED4E74 5B0A3DB5 C6C29A8B F04B19EC
         051F3BA9 A2F320F8 6B7DEFA2 FDE8C627 8E108B36 E595FC1A




-------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
NonceU is
```

```
              00 774E07FF C5A3A7A8 85D16C4E F49F9380 91B49314


NonceV is
              01 9AA2022D EAB805FA 2BA8044F BDAFBDDA 71D688D8


Z is
              00 92361CC1 B0B2D3F7 F5A0B498 4D101CA7 0559AEB9


OtherInfo is
             1234 56789ABC DEF0414C 49434531 3233A300 774E07FF
         C5A3A7A8 85D16C4E F49F9380 91B49314 424F4242 59343536


DerivedKeyMaterial is
                                                             E3FF
         906CE89A 8BD2A61C C4ED4E74 5B0A3DB5 C6C29A8B F04B19EC
         051F3BA9 A2F320F8 6B7DEFA2 FDE8C627 8E108B36 E595FC1A


U2V
----------------
MacData is
                                       4B43 5F325F55 414C4943
         45424F42 42590077 4E07FFC5 A3A7A885 D16C4EF4 9F938091
         B4931401 9AA2022D EAB805FA 2BA8044F BDAFBDDA 71D688D8


MacKey is
                                       E3FF 906CE89A 8BD2A61C


Mtag is
                  B45C5AC6 31A968BF 660FE014 5440833A 661A4771


V2U
----------------
MacData is
                                       4B43 5F325F56 424F4242
         59414C49 4345019A A2022DEA B805FA2B A8044FBD AFBDDA71
         D688D800 774E07FF C5A3A7A8 85D16C4E F49F9380 91B49314
```

MacKey is
E3FF 906CE89A 8BD2A61C

Mtag is
CC20D79F 51C78F69 80C90E5F 1E96C14F 2B4DE2D0

KeyData is
C4ED4E74 5B0A3DB5 C6C29A8B F04B19EC
051F3BA9 A2F320F8 6B7DEFA2 FDE8C627 8E108B36 E595FC1A

FullUnifiedCDH(K-233)
----
dsU is
                                                    003B 2C490A0D
        5C0F2219 77BFBE9D 4F51867F AB0F7CFE 68B4365E E9CF7AD1

QsU_x is
                                                    0156 B2CDDB11
        3BB74CBD CB3706DC 4C638C6D 840E5F9A F515AE31 75CD5DDD

QsU_y is
                                                    01DC AFB9C12C
        0CC9F5F7 52A39362 B0AB7164 B3CD80B9 B735600B 7573CBA2

dsV is
                                                    005A 4315263C
        7D4BE3DE AD91C0F9 C2F1A7D9 519E3859 950B76C3 9A11178A

QsV_x is
                                                    009E F05D57EC
        BB782884 174548EB A14C003D B8CD60CF FFE9B81B 8532B778

QsV_y is
                                                    000E 16BF3F5C
        4FB65307 56B0169B 1603993C 4254A744 C0FA50DA D65D72C7

deU is
                                                    003C 5D3A78CF
        F9570D5B 1E95E699 03C435ED 56C376F1 0F31BE66 E0A06AB1

QeU_x is
                                                    0004 2FC887C3
        3B87253E E7F6A0D1 73C2E11D 13C0DACC 78A0248C EFD3947B

QeU_y is
                                                    01A2 6597DDC8

```
        5E9177DD FB840ABB E06F4792 1DCC4B39 7767CB01 792108EF


deV is
                                                    0064 5ABB6464
        E24E03E7 F2554AD4 7AD25973 1C32217D 528A8353 B4583CEE


QeV_x is
                                                    01AB 6C02D3B0
        18689C77 6219F70E 05EF935B C8C4D166 6D5A779B 6942C084


QeV_y is
                                                    01E2 BA4340C7
        24497C39 2E4D1A18 E23C76F8 6BE6C22B 7355D1EF AC4E3143




------------------------------------------------------------
no Key Confirmation
Zs is
                                                    0198 B09EF82A
        398C0B2F 0CDFB640 AE2D671F AF7E0068 0CB66813 075A2424


Ze is
                                                    001D DC51EB59
        A576641F 08ECD16A 10B58A4E C6538B5F 223C2ED1 D2725112


Z is
                                  001DDC51 EB59A576 641F08EC
        D16A10B5 8A4EC653 8B5F223C 2ED1D272 51120198 B09EF82A
        398C0B2F 0CDFB640 AE2D671F AF7E0068 0CB66813 075A2424


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                AD5B56EC A39ADAE0
        29727529 C9826006 B5185038 7FE9D405 4EF4A69C 626F517D
        006DA50C E1431E81 904C7BE7 114F9F85 F681FA76 2D2805C5
```

KeyData is
                                                AD5B56EC A39ADAE0
        29727529 C9826006 B5185038 7FE9D405 4EF4A69C 626F517D
        006DA50C E1431E81 904C7BE7 114F9F85 F681FA76 2D2805C5

Scheme Initiator, Key Confirmation Provider: U to V
Zs is
                                                    0198 B09EF82A
        398C0B2F 0CDFB640 AE2D671F AF7E0068 0CB66813 075A2424

Ze is
                                                    001D DC51EB59
        A576641F 08ECD16A 10B58A4E C6538B5F 223C2ED1 D2725112

Z is
                                    001DDC51 EB59A576 641F08EC
        D16A10B5 8A4EC653 8B5F223C 2ED1D272 51120198 B09EF82A
        398C0B2F 0CDFB640 AE2D671F AF7E0068 0CB66813 075A2424

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
            AD5B 56ECA39A DAE02972 7529C982 6006B518 50387FE9
        D4054EF4 A69C626F 517D006D A50CE143 1E81904C 7BE7114F
        9F85F681 FA762D28 05C57C81 31CB6B6F 99AB2595 9B9BCA93

MacData is
                          4B435F31 5F55414C 49434542 4F424259
        00042FC8 87C33B87 253EE7F6 A0D173C2 E11D13C0 DACC78A0
        248CEFD3 947B01A2 6597DDC8 5E9177DD FB840ABB E06F4792
        1DCC4B39 7767CB01 792108EF 01AB6C02 D3B01868 9C776219
        F70E05EF 935BC8C4 D1666D5A 779B6942 C08401E2 BA4340C7
        24497C39 2E4D1A18 E23C76F8 6BE6C22B 7355D1EF AC4E3143

```
MacKey is
                              AD5B 56ECA39A DAE02972 7529C982


Mtag is
                                                        8C40242A
        F7577713 474A4EDF 3365C6AF 2AE8501F 77D7C221 7245258E


KeyData is
                                               6006B518 50387FE9
        D4054EF4 A69C626F 517D006D A50CE143 1E81904C 7BE7114F
        9F85F681 FA762D28 05C57C81 31CB6B6F 99AB2595 9B9BCA93




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Zs is
                                                   0198 B09EF82A
        398C0B2F 0CDFB640 AE2D671F AF7E0068 0CB66813 075A2424


Ze is
                                                   001D DC51EB59
        A576641F 08ECD16A 10B58A4E C6538B5F 223C2ED1 D2725112


Z is
                                    001DDC51 EB59A576 641F08EC
        D16A10B5 8A4EC653 8B5F223C 2ED1D272 51120198 B09EF82A
        398C0B2F 0CDFB640 AE2D671F AF7E0068 0CB66813 075A2424


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            AD5B 56ECA39A DAE02972 7529C982 6006B518 50387FE9
        D4054EF4 A69C626F 517D006D A50CE143 1E81904C 7BE7114F
        9F85F681 FA762D28 05C57C81 31CB6B6F 99AB2595 9B9BCA93
```

MacData is
                        4B435F31 5F56424F 42425941 4C494345
        01AB6C02 D3B01868 9C776219 F70E05EF 935BC8C4 D1666D5A
        779B6942 C08401E2 BA4340C7 24497C39 2E4D1A18 E23C76F8
        6BE6C22B 7355D1EF AC4E3143 00042FC8 87C33B87 253EE7F6
        A0D173C2 E11D13C0 DACC78A0 248CEFD3 947B01A2 6597DDC8
        5E9177DD FB840ABB E06F4792 1DCC4B39 7767CB01 792108EF

MacKey is
                            AD5B 56ECA39A DAE02972 7529C982

Mtag is
                                                    4EC522C5
        CBD2C6A0 0828FB8D 5E141E97 7E8E48C2 D9D2936C F3F506BE

KeyData is
                                                6006B518 50387FE9
        D4054EF4 A69C626F 517D006D A50CE143 1E81904C 7BE7114F
        9F85F681 FA762D28 05C57C81 31CB6B6F 99AB2595 9B9BCA93

Scheme Initiator, Key Confirmation Bilateral
Zs is
                                                    0198 B09EF82A
        398C0B2F 0CDFB640 AE2D671F AF7E0068 0CB66813 075A2424

Ze is
                                                    001D DC51EB59
        A576641F 08ECD16A 10B58A4E C6538B5F 223C2ED1 D2725112

Z is
                                 001DDC51 EB59A576 641F08EC
        D16A10B5 8A4EC653 8B5F223C 2ED1D272 51120198 B09EF82A
        398C0B2F 0CDFB640 AE2D671F AF7E0068 0CB66813 075A2424

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

```
DerivedKeyMaterial is
            AD5B 56ECA39A DAE02972 7529C982 6006B518 50387FE9
         D4054EF4 A69C626F 517D006D A50CE143 1E81904C 7BE7114F
         9F85F681 FA762D28 05C57C81 31CB6B6F 99AB2595 9B9BCA93


U2V
----------------
MacData is
                         4B435F32 5F55414C 49434542 4F424259
         00042FC8 87C33B87 253EE7F6 A0D173C2 E11D13C0 DACC78A0
         248CEFD3 947B01A2 6597DDC8 5E9177DD FB840ABB E06F4792
         1DCC4B39 7767CB01 792108EF 01AB6C02 D3B01868 9C776219
         F70E05EF 935BC8C4 D1666D5A 779B6942 C08401E2 BA4340C7
         24497C39 2E4D1A18 E23C76F8 6BE6C22B 7355D1EF AC4E3143


MacKey is
                              AD5B 56ECA39A DAE02972 7529C982


Mtag is
                                                      33E5B34F
         E4B9629E 0461157F 39345413 0E7DC3BB C44464CA B652C606


V2U
----------------
MacData is
                         4B435F32 5F56424F 42425941 4C494345
         01AB6C02 D3B01868 9C776219 F70E05EF 935BC8C4 D1666D5A
         779B6942 C08401E2 BA4340C7 24497C39 2E4D1A18 E23C76F8
         6BE6C22B 7355D1EF AC4E3143 00042FC8 87C33B87 253EE7F6
         A0D173C2 E11D13C0 DACC78A0 248CEFD3 947B01A2 6597DDC8
         5E9177DD FB840ABB E06F4792 1DCC4B39 7767CB01 792108EF


MacKey is
                              AD5B 56ECA39A DAE02972 7529C982


Mtag is
                                                      30E9E908
         0C949F03 51F734BA 6C3A2772 559D6738 EF543BE0 639C8BA5
```

KeyData is
                                                6006B518 50387FE9
        D4054EF4 A69C626F 517D006D A50CE143 1E81904C 7BE7114F
        9F85F681 FA762D28 05C57C81 31CB6B6F 99AB2595 9B9BCA93

FullMQV(K-233)
----
dsU is
                                                    003B 2C490A0D
        5C0F2219 77BFBE9D 4F51867F AB0F7CFE 68B4365E E9CF7AD1

QsU_x is
                                                    0156 B2CDDB11
        3BB74CBD CB3706DC 4C638C6D 840E5F9A F515AE31 75CD5DDD

QsU_y is
                                                    01DC AFB9C12C
        0CC9F5F7 52A39362 B0AB7164 B3CD80B9 B735600B 7573CBA2

dsV is
                                                    005A 4315263C
        7D4BE3DE AD91C0F9 C2F1A7D9 519E3859 950B76C3 9A11178A

QsV_x is
                                                    009E F05D57EC
        BB782884 174548EB A14C003D B8CD60CF FFE9B81B 8532B778

QsV_y is
                                                    000E 16BF3F5C
        4FB65307 56B0169B 1603993C 4254A744 C0FA50DA D65D72C7

deU is
                                                    003C 5D3A78CF
        F9570D5B 1E95E699 03C435ED 56C376F1 0F31BE66 E0A06AB1

```
QeU_x is
                                                    0004 2FC887C3
        3B87253E E7F6A0D1 73C2E11D 13C0DACC 78A0248C EFD3947B


QeU_y is
                                                    01A2 6597DDC8
        5E9177DD FB840ABB E06F4792 1DCC4B39 7767CB01 792108EF


deV is
                                                    0064 5ABB6464
        E24E03E7 F2554AD4 7AD25973 1C32217D 528A8353 B4583CEE


QeV_x is
                                                    01AB 6C02D3B0
        18689C77 6219F70E 05EF935B C8C4D166 6D5A779B 6942C084


QeV_y is
                                                    01E2 BA4340C7
        24497C39 2E4D1A18 E23C76F8 6BE6C22B 7355D1EF AC4E3143




------------------------------------------------------------
no Key Confirmation
Z is
                                                    01DF CE36BC8C
        BFDE6D6F 9DAC89B6 0B217A16 5B02383C 65D45E76 A5C4EE27


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                  D6F145F1 3A0BB20A
        CB881B6C A31EA8BB 8C5D6DA2 30FCE4B9 D3B01DD9 D2035FD9
        31EA7E3A 5D5E7AAF F98C1262 43E31C16 3A95F9B3 63D63E28


KeyData is
```

```
                                                  D6F145F1 3A0BB20A
        CB881B6C A31EA8BB 8C5D6DA2 30FCE4B9 D3B01DD9 D2035FD9
        31EA7E3A 5D5E7AAF F98C1262 43E31C16 3A95F9B3 63D63E28



------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Z is
                                                     01DF CE36BC8C
        BFDE6D6F 9DAC89B6 0B217A16 5B02383C 65D45E76 A5C4EE27


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            D6F1 45F13A0B B20ACB88 1B6CA31E A8BB8C5D 6DA230FC
        E4B9D3B0 1DD9D203 5FD931EA 7E3A5D5E 7AAFF98C 126243E3
        1C163A95 F9B363D6 3E28AAC9 FB3F0328 5E3809CD ECE9C163


MacData is
                         4B435F31 5F55414C 49434542 4F424259
        00042FC8 87C33B87 253EE7F6 A0D173C2 E11D13C0 DACC78A0
        248CEFD3 947B01A2 6597DDC8 5E9177DD FB840ABB E06F4792
        1DCC4B39 7767CB01 792108EF 01AB6C02 D3B01868 9C776219
        F70E05EF 935BC8C4 D1666D5A 779B6942 C08401E2 BA4340C7
        24497C39 2E4D1A18 E23C76F8 6BE6C22B 7355D1EF AC4E3143


MacKey is
                              D6F1 45F13A0B B20ACB88 1B6CA31E


Mtag is
                                                        C1738B47
        2A04A806 CA887559 AD79C286 9F50231F 05F2172F F6E2B160


KeyData is
                                                  A8BB8C5D 6DA230FC
        E4B9D3B0 1DD9D203 5FD931EA 7E3A5D5E 7AAFF98C 126243E3
        1C163A95 F9B363D6 3E28AAC9 FB3F0328 5E3809CD ECE9C163
```

```
-----------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
                                                 01DF CE36BC8C
        BFDE6D6F 9DAC89B6 0B217A16 5B02383C 65D45E76 A5C4EE27


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            D6F1 45F13A0B B20ACB88 1B6CA31E A8BB8C5D 6DA230FC
        E4B9D3B0 1DD9D203 5FD931EA 7E3A5D5E 7AAFF98C 126243E3
        1C163A95 F9B363D6 3E28AAC9 FB3F0328 5E3809CD ECE9C163


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        01AB6C02 D3B01868 9C776219 F70E05EF 935BC8C4 D1666D5A
        779B6942 C08401E2 BA4340C7 24497C39 2E4D1A18 E23C76F8
        6BE6C22B 7355D1EF AC4E3143 00042FC8 87C33B87 253EE7F6
        A0D173C2 E11D13C0 DACC78A0 248CEFD3 947B01A2 6597DDC8
        5E9177DD FB840ABB E06F4792 1DCC4B39 7767CB01 792108EF


MacKey is
                             D6F1 45F13A0B B20ACB88 1B6CA31E


Mtag is
                                                     0796CB13
        A7D93E42 2629AEBD B4B1C9C2 DD7462E3 6D71B8CC 2A995691


KeyData is
                                                 A8BB8C5D 6DA230FC
        E4B9D3B0 1DD9D203 5FD931EA 7E3A5D5E 7AAFF98C 126243E3
        1C163A95 F9B363D6 3E28AAC9 FB3F0328 5E3809CD ECE9C163
```

```
-----------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
Z is
                                                    01DF CE36BC8C
        BFDE6D6F 9DAC89B6 0B217A16 5B02383C 65D45E76 A5C4EE27


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            D6F1 45F13A0B B20ACB88 1B6CA31E A8BB8C5D 6DA230FC
        E4B9D3B0 1DD9D203 5FD931EA 7E3A5D5E 7AAFF98C 126243E3
        1C163A95 F9B363D6 3E28AAC9 FB3F0328 5E3809CD ECE9C163


U2V
----------------
MacData is
                         4B435F32 5F55414C 49434542 4F424259
        00042FC8 87C33B87 253EE7F6 A0D173C2 E11D13C0 DACC78A0
        248CEFD3 947B01A2 6597DDC8 5E9177DD FB840ABB E06F4792
        1DCC4B39 7767CB01 792108EF 01AB6C02 D3B01868 9C776219
        F70E05EF 935BC8C4 D1666D5A 779B6942 C08401E2 BA4340C7
        24497C39 2E4D1A18 E23C76F8 6BE6C22B 7355D1EF AC4E3143


MacKey is
                             D6F1 45F13A0B B20ACB88 1B6CA31E


Mtag is
                                                    5CF83EA0
        1825CCF0 FF4EF495 CC79FD30 4FCC8210 7475B7FE 261D1477


V2U
----------------
MacData is
                         4B435F32 5F56424F 42425941 4C494345
        01AB6C02 D3B01868 9C776219 F70E05EF 935BC8C4 D1666D5A
        779B6942 C08401E2 BA4340C7 24497C39 2E4D1A18 E23C76F8
        6BE6C22B 7355D1EF AC4E3143 00042FC8 87C33B87 253EE7F6
```

```
        A0D173C2 E11D13C0 DACC78A0 248CEFD3 947B01A2 6597DDC8
        5E9177DD FB840ABB E06F4792 1DCC4B39 7767CB01 792108EF


MacKey is
                             D6F1 45F13A0B B20ACB88 1B6CA31E


Mtag is
                                                    5E2EDB24
        BF8681EF 86E429A9 A02040F0 C4CFC8A0 AF42D10F B7411846


KeyData is
                                               A8BB8C5D 6DA230FC
        E4B9D3B0 1DD9D203 5FD931EA 7E3A5D5E 7AAFF98C 126243E3
        1C163A95 F9B363D6 3E28AAC9 FB3F0328 5E3809CD ECE9C163




EphemeralUnifiedCDH(K-233)
------------------------------------------------------------
deU is
                                                   003C 5D3A78CF
        F9570D5B 1E95E699 03C435ED 56C376F1 0F31BE66 E0A06AB1


QeU_x is
                                                   0004 2FC887C3
        3B87253E E7F6A0D1 73C2E11D 13C0DACC 78A0248C EFD3947B


QeU_y is
                                                   01A2 6597DDC8
        5E9177DD FB840ABB E06F4792 1DCC4B39 7767CB01 792108EF


deV is
                                                   0064 5ABB6464
        E24E03E7 F2554AD4 7AD25973 1C32217D 528A8353 B4583CEE


QeV_x is
                                                   01AB 6C02D3B0
        18689C77 6219F70E 05EF935B C8C4D166 6D5A779B 6942C084
```

```
QeV_y is
                                                    01E2 BA4340C7
        24497C39 2E4D1A18 E23C76F8 6BE6C22B 7355D1EF AC4E3143




------------------------------------------------------------
no Key Confirmation
Z is
                                                    001D DC51EB59
        A576641F 08ECD16A 10B58A4E C6538B5F 223C2ED1 D2725112


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                43C739D6 EABEA94D
        60979AE1 D5C8C6A4 70AB0101 991B13D2 C71D4696 FE43F873
        C69F53D0 AEB4EB53 56613FAE 43BA0F6F EAC2912E B9817323


KeyData is
                                                43C739D6 EABEA94D
        60979AE1 D5C8C6A4 70AB0101 991B13D2 C71D4696 FE43F873
        C69F53D0 AEB4EB53 56613FAE 43BA0F6F EAC2912E B9817323




OnePassUnifiedCDH(K-233)
------------------------------------------------------------
dsU is
                                                    003B 2C490A0D
        5C0F2219 77BFBE9D 4F51867F AB0F7CFE 68B4365E E9CF7AD1


QsU_x is
                                                    0156 B2CDDB11
        3BB74CBD CB3706DC 4C638C6D 840E5F9A F515AE31 75CD5DDD
```

QsU_y is
                                                    01DC AFB9C12C
        0CC9F5F7 52A39362 B0AB7164 B3CD80B9 B735600B 7573CBA2

dsV is
                                                    005A 4315263C
        7D4BE3DE AD91C0F9 C2F1A7D9 519E3859 950B76C3 9A11178A

QsV_x is
                                                    009E F05D57EC
        BB782884 174548EB A14C003D B8CD60CF FFE9B81B 8532B778

QsV_y is
                                                    000E 16BF3F5C
        4FB65307 56B0169B 1603993C 4254A744 C0FA50DA D65D72C7

deU is
                                                    003C 5D3A78CF
        F9570D5B 1E95E699 03C435ED 56C376F1 0F31BE66 E0A06AB1

QeU_x is
                                                    0004 2FC887C3
        3B87253E E7F6A0D1 73C2E11D 13C0DACC 78A0248C EFD3947B

QeU_y is
                                                    01A2 6597DDC8
        5E9177DD FB840ABB E06F4792 1DCC4B39 7767CB01 792108EF

---
no Key Confirmation
Zs is
                                                    0198 B09EF82A
        398C0B2F 0CDFB640 AE2D671F AF7E0068 0CB66813 075A2424

Ze is
                                                    015A DB6BA602

```
        D97FABDE 64186020 F8E1B02D 43561F37 9D3A43A6 8995C47E


Z is
                                  015ADB6B A602D97F ABDE6418
        6020F8E1 B02D4356 1F379D3A 43A68995 C47E0198 B09EF82A
        398C0B2F 0CDFB640 AE2D671F AF7E0068 0CB66813 075A2424


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                             D406A6C8 8D8984D1
        304F8AD5 F9E80D30 48675655 FBB2B5FC 1BDBC195 F44EE8EF
        019C021B 00F1361B 952F7EE9 B8261DF4 AF112812 EE84A492


KeyData is
                                             D406A6C8 8D8984D1
        304F8AD5 F9E80D30 48675655 FBB2B5FC 1BDBC195 F44EE8EF
        019C021B 00F1361B 952F7EE9 B8261DF4 AF112812 EE84A492




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                                                 004D 56F9346A
        8B9C90B5 565EB261 F794D585 DB224A4C 3AB2C154 8CF1416D


Zs is
                                                 0198 B09EF82A
        398C0B2F 0CDFB640 AE2D671F AF7E0068 0CB66813 075A2424


Ze is
                                                 015A DB6BA602
        D97FABDE 64186020 F8E1B02D 43561F37 9D3A43A6 8995C47E


Z is
                                  015ADB6B A602D97F ABDE6418
```

```
        6020F8E1 B02D4356 1F379D3A 43A68995 C47E0198 B09EF82A
        398C0B2F 0CDFB640 AE2D671F AF7E0068 0CB66813 075A2424


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            D406 A6C88D89 84D1304F 8AD5F9E8 0D304867 5655FBB2
        B5FC1BDB C195F44E E8EF019C 021B00F1 361B952F 7EE9B826
        1DF4AF11 2812EE84 A4921714 49CCC8C7 B19C2E7A 0C0A9C26


MacData is
                                        4B43 5F315F55 414C4943
        45424F42 42590004 2FC887C3 3B87253E E7F6A0D1 73C2E11D
        13C0DACC 78A0248C EFD3947B 01A26597 DDC85E91 77DDFB84
        0ABBE06F 47921DCC 4B397767 CB017921 08EF004D 56F9346A
        8B9C90B5 565EB261 F794D585 DB224A4C 3AB2C154 8CF1416D


MacKey is
                               D406 A6C88D89 84D1304F 8AD5F9E8


Mtag is
                                                        50A3FF77
        84B06C38 D7C63732 97EDC2EA 01D786E1 08C2FF42 4059A6C4


KeyData is
                                                0D304867 5655FBB2
        B5FC1BDB C195F44E E8EF019C 021B00F1 361B952F 7EE9B826
        1DF4AF11 2812EE84 A4921714 49CCC8C7 B19C2E7A 0C0A9C26




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
                                                    004D 56F9346A
        8B9C90B5 565EB261 F794D585 DB224A4C 3AB2C154 8CF1416D
```

```
Zs is
                                                  0198 B09EF82A
        398C0B2F 0CDFB640 AE2D671F AF7E0068 0CB66813 075A2424


Ze is
                                                  015A DB6BA602
        D97FABDE 64186020 F8E1B02D 43561F37 9D3A43A6 8995C47E


Z is
                                  015ADB6B A602D97F ABDE6418
        6020F8E1 B02D4356 1F379D3A 43A68995 C47E0198 B09EF82A
        398C0B2F 0CDFB640 AE2D671F AF7E0068 0CB66813 075A2424


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            D406 A6C88D89 84D1304F 8AD5F9E8 0D304867 5655FBB2
        B5FC1BDB C195F44E E8EF019C 021B00F1 361B952F 7EE9B826
        1DF4AF11 2812EE84 A4921714 49CCC8C7 B19C2E7A 0C0A9C26


MacData is
                                                    4B435F31
        5F56424F 42425941 4C494345 00042FC8 87C33B87 253EE7F6
        A0D173C2 E11D13C0 DACC78A0 248CEFD3 947B01A2 6597DDC8
        5E9177DD FB840ABB E06F4792 1DCC4B39 7767CB01 792108EF


MacKey is
                             D406 A6C88D89 84D1304F 8AD5F9E8


Mtag is
                                                    A3EE87A6
        66E4F208 72A5DE21 6865ACBD FBC39CB9 237E7DAD 7F66D6AB


KeyData is
                                                  0D304867 5655FBB2
        B5FC1BDB C195F44E E8EF019C 021B00F1 361B952F 7EE9B826
        1DF4AF11 2812EE84 A4921714 49CCC8C7 B19C2E7A 0C0A9C26
```

```
------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
                                                  004D 56F9346A
        8B9C90B5 565EB261 F794D585 DB224A4C 3AB2C154 8CF1416D


Zs is
                                                  0198 B09EF82A
        398C0B2F 0CDFB640 AE2D671F AF7E0068 0CB66813 075A2424


Ze is
                                                  015A DB6BA602
        D97FABDE 64186020 F8E1B02D 43561F37 9D3A43A6 8995C47E


Z is
                                  015ADB6B A602D97F ABDE6418
        6020F8E1 B02D4356 1F379D3A 43A68995 C47E0198 B09EF82A
        398C0B2F 0CDFB640 AE2D671F AF7E0068 0CB66813 075A2424


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            D406 A6C88D89 84D1304F 8AD5F9E8 0D304867 5655FBB2
        B5FC1BDB C195F44E E8EF019C 021B00F1 361B952F 7EE9B826
        1DF4AF11 2812EE84 A4921714 49CCC8C7 B19C2E7A 0C0A9C26


U2V
----------------
MacData is
                                      4B43 5F325F55 414C4943
        45424F42 42590004 2FC887C3 3B87253E E7F6A0D1 73C2E11D
        13C0DACC 78A0248C EFD3947B 01A26597 DDC85E91 77DDFB84
        0ABBE06F 47921DCC 4B397767 CB017921 08EF004D 56F9346A
        8B9C90B5 565EB261 F794D585 DB224A4C 3AB2C154 8CF1416D
```

```
MacKey is
                              D406 A6C88D89 84D1304F 8AD5F9E8


Mtag is
                                                        7F0E5086
        8BD055BC C3EFF384 F0B6DFFC 9C062AEA 8FB6E0C2 94CEF151


V2U
----------------
MacData is
                                       4B43 5F325F56 424F4242
        59414C49 4345004D 56F9346A 8B9C90B5 565EB261 F794D585
        DB224A4C 3AB2C154 8CF1416D 00042FC8 87C33B87 253EE7F6
        A0D173C2 E11D13C0 DACC78A0 248CEFD3 947B01A2 6597DDC8
        5E9177DD FB840ABB E06F4792 1DCC4B39 7767CB01 792108EF


MacKey is
                              D406 A6C88D89 84D1304F 8AD5F9E8


Mtag is
                                                        2948B9F0
        BCCD1E35 3CCBB739 BA236DEF 3303303A E5BFBF05 00773EA6


KeyData is
                                                0D304867 5655FBB2
        B5FC1BDB C195F44E E8EF019C 021B00F1 361B952F 7EE9B826
        1DF4AF11 2812EE84 A4921714 49CCC8C7 B19C2E7A 0C0A9C26




OnePassMQV(K-233)
------------------------------------------------------------
dsU is
                                                    003B 2C490A0D
        5C0F2219 77BFBE9D 4F51867F AB0F7CFE 68B4365E E9CF7AD1


QsU_x is
                                                    0156 B2CDDB11
```

3BB74CBD CB3706DC 4C638C6D 840E5F9A F515AE31 75CD5DDD

QsU_y is
01DC AFB9C12C
0CC9F5F7 52A39362 B0AB7164 B3CD80B9 B735600B 7573CBA2

dsV is
005A 4315263C
7D4BE3DE AD91C0F9 C2F1A7D9 519E3859 950B76C3 9A11178A

QsV_x is
009E F05D57EC
BB782884 174548EB A14C003D B8CD60CF FFE9B81B 8532B778

QsV_y is
000E 16BF3F5C
4FB65307 56B0169B 1603993C 4254A744 C0FA50DA D65D72C7

deU is
003C 5D3A78CF
F9570D5B 1E95E699 03C435ED 56C376F1 0F31BE66 E0A06AB1

QeU_x is
0004 2FC887C3
3B87253E E7F6A0D1 73C2E11D 13C0DACC 78A0248C EFD3947B

QeU_y is
01A2 6597DDC8
5E9177DD FB840ABB E06F4792 1DCC4B39 7767CB01 792108EF

---

no Key Confirmation
Z is
00C1 CCD3994C
1FDB6B3D 50CFA4A2 2710833E 5FAE2FD5 4B8FD929 BF0ABDF8

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                F96C8B5B B6BB1127
        BBCD1A44 C8817555 0FBC9E89 A1C29DA5 CAFE4F7D 720F16C8
        7FC520CA D1C76F26 BA3E9B78 E951E96B E1B32CAE F1C47207


KeyData is
                                                F96C8B5B B6BB1127
        BBCD1A44 C8817555 0FBC9E89 A1C29DA5 CAFE4F7D 720F16C8
        7FC520CA D1C76F26 BA3E9B78 E951E96B E1B32CAE F1C47207




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                                                    004D 56F9346A
        8B9C90B5 565EB261 F794D585 DB224A4C 3AB2C154 8CF1416D


Z is
                                                    00C1 CCD3994C
        1FDB6B3D 50CFA4A2 2710833E 5FAE2FD5 4B8FD929 BF0ABDF8


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            F96C 8B5BB6BB 1127BBCD 1A44C881 75550FBC 9E89A1C2
        9DA5CAFE 4F7D720F 16C87FC5 20CAD1C7 6F26BA3E 9B78E951
        E96BE1B3 2CAEF1C4 7207DE44 5C5DAFE8 BC0E5637 D1B5C1CA


MacData is
                                        4B43 5F315F55 414C4943
        45424F42 42590004 2FC887C3 3B87253E E7F6A0D1 73C2E11D
        13C0DACC 78A0248C EFD3947B 01A26597 DDC85E91 77DDFB84
        0ABBE06F 47921DCC 4B397767 CB017921 08EF004D 56F9346A
```

8B9C90B5 565EB261 F794D585 DB224A4C 3AB2C154 8CF1416D

MacKey is
F96C 8B5BB6BB 1127BBCD 1A44C881

Mtag is
7C5B3006
CA5A462D D32B9CEC 85604635 8886A390 4F7D6447 176C0FCA

KeyData is
75550FBC 9E89A1C2
9DA5CAFE 4F7D720F 16C87FC5 20CAD1C7 6F26BA3E 9B78E951
E96BE1B3 2CAEF1C4 7207DE44 5C5DAFE8 BC0E5637 D1B5C1CA

Scheme Responder, Key Confirmation Provider: V to U
NonceU is
004D 56F9346A
8B9C90B5 565EB261 F794D585 DB224A4C 3AB2C154 8CF1416D

Z is
00C1 CCD3994C
1FDB6B3D 50CFA4A2 2710833E 5FAE2FD5 4B8FD929 BF0ABDF8

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
F96C 8B5BB6BB 1127BBCD 1A44C881 75550FBC 9E89A1C2
9DA5CAFE 4F7D720F 16C87FC5 20CAD1C7 6F26BA3E 9B78E951
E96BE1B3 2CAEF1C4 7207DE44 5C5DAFE8 BC0E5637 D1B5C1CA

MacData is
4B435F31
5F56424F 42425941 4C494345 00042FC8 87C33B87 253EE7F6
A0D173C2 E11D13C0 DACC78A0 248CEFD3 947B01A2 6597DDC8

```
        5E9177DD FB840ABB E06F4792 1DCC4B39 7767CB01 792108EF


MacKey is
                              F96C 8B5BB6BB 1127BBCD 1A44C881


Mtag is
                                                        C4541CD7
        C21FC380 110FF458 F4A9E83E F646240E 7414A67F B898A463


KeyData is
                                                   75550FBC 9E89A1C2
        9DA5CAFE 4F7D720F 16C87FC5 20CAD1C7 6F26BA3E 9B78E951
        E96BE1B3 2CAEF1C4 7207DE44 5C5DAFE8 BC0E5637 D1B5C1CA




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
                                                      004D 56F9346A
        8B9C90B5 565EB261 F794D585 DB224A4C 3AB2C154 8CF1416D


Z is
                                                      00C1 CCD3994C
        1FDB6B3D 50CFA4A2 2710833E 5FAE2FD5 4B8FD929 BF0ABDF8


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            F96C 8B5BB6BB 1127BBCD 1A44C881 75550FBC 9E89A1C2
        9DA5CAFE 4F7D720F 16C87FC5 20CAD1C7 6F26BA3E 9B78E951
        E96BE1B3 2CAEF1C4 7207DE44 5C5DAFE8 BC0E5637 D1B5C1CA


U2V
----------------
MacData is
                                       4B43 5F325F55 414C4943
```

```
        45424F42 42590004 2FC887C3 3B87253E E7F6A0D1 73C2E11D
        13C0DACC 78A0248C EFD3947B 01A26597 DDC85E91 77DDFB84
        0ABBE06F 47921DCC 4B397767 CB017921 08EF004D 56F9346A
        8B9C90B5 565EB261 F794D585 DB224A4C 3AB2C154 8CF1416D


MacKey is
                             F96C 8B5BB6BB 1127BBCD 1A44C881


Mtag is
                                                      7B0D6C6D
        5D5F3616 A26869A5 AA630EA0 86DC739E 28FFA165 4E88D3F4


V2U
----------------
MacData is
                                       4B43 5F325F56 424F4242
        59414C49 4345004D 56F9346A 8B9C90B5 565EB261 F794D585
        DB224A4C 3AB2C154 8CF1416D 00042FC8 87C33B87 253EE7F6
        A0D173C2 E11D13C0 DACC78A0 248CEFD3 947B01A2 6597DDC8
        5E9177DD FB840ABB E06F4792 1DCC4B39 7767CB01 792108EF


MacKey is
                             F96C 8B5BB6BB 1127BBCD 1A44C881


Mtag is
                                                      C6DBAD12
        7CD4BBB1 6375C7BC 7974B869 5A3284DC 8A569702 2B88A4E5


KeyData is
                                                 75550FBC 9E89A1C2
        9DA5CAFE 4F7D720F 16C87FC5 20CAD1C7 6F26BA3E 9B78E951
        E96BE1B3 2CAEF1C4 7207DE44 5C5DAFE8 BC0E5637 D1B5C1CA




OnePassDiffieHellmanCDH(K-233)
------------------------------------------------------------
dsV is
                                                    005A 4315263C
```

```
        7D4BE3DE AD91C0F9 C2F1A7D9 519E3859 950B76C3 9A11178A


QsV_x is
                                                  009E F05D57EC
        BB782884 174548EB A14C003D B8CD60CF FFE9B81B 8532B778


QsV_y is
                                                  000E 16BF3F5C
        4FB65307 56B0169B 1603993C 4254A744 C0FA50DA D65D72C7


deU is
                                                  003C 5D3A78CF
        F9570D5B 1E95E699 03C435ED 56C376F1 0F31BE66 E0A06AB1


QeU_x is
                                                  0004 2FC887C3
        3B87253E E7F6A0D1 73C2E11D 13C0DACC 78A0248C EFD3947B


QeU_y is
                                                  01A2 6597DDC8
        5E9177DD FB840ABB E06F4792 1DCC4B39 7767CB01 792108EF




------------------------------------------------------------
no Key Confirmation
Z is
                                                  015A DB6BA602
        D97FABDE 64186020 F8E1B02D 43561F37 9D3A43A6 8995C47E


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                  B79B7CDB 945FE409
        5B62F335 A43C5B1B EF4AEC6D FA4732D8 34E5EC01 FB549BA7
        8A45790E D5B1388F D0F8CE1F BA95B933 28B4D916 391F6A0A
```

KeyData is
                                                B79B7CDB 945FE409
        5B62F335 A43C5B1B EF4AEC6D FA4732D8 34E5EC01 FB549BA7
        8A45790E D5B1388F D0F8CE1F BA95B933 28B4D916 391F6A0A

Scheme Responder, Key Confirmation Provider: V to U
Z is
                                                    015A DB6BA602
        D97FABDE 64186020 F8E1B02D 43561F37 9D3A43A6 8995C47E

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
            B79B 7CDB945F E4095B62 F335A43C 5B1BEF4A EC6DFA47
        32D834E5 EC01FB54 9BA78A45 790ED5B1 388FD0F8 CE1FBA95
        B93328B4 D916391F 6A0AA5F9 E2C093B3 CFFA1A2A DE49F08A

MacData is
                                                        4B435F31
        5F56424F 42425941 4C494345 00042FC8 87C33B87 253EE7F6
        A0D173C2 E11D13C0 DACC78A0 248CEFD3 947B01A2 6597DDC8
        5E9177DD FB840ABB E06F4792 1DCC4B39 7767CB01 792108EF

MacKey is
                              B79B 7CDB945F E4095B62 F335A43C

Mtag is
                                                        AB3D2B77
        7969F954 248AFD3D B24DBCAD 57D9B1D2 E669E8FA FC858207

KeyData is
                                                5B1BEF4A EC6DFA47
        32D834E5 EC01FB54 9BA78A45 790ED5B1 388FD0F8 CE1FBA95
        B93328B4 D916391F 6A0AA5F9 E2C093B3 CFFA1A2A DE49F08A

StaticUnifiedCDH(K-233)
---
dsU is
0035 CDEA69F4
6DA05C54 3081273B 2E5F00F5 1DF7195D A6E8DAE8 C08B650B

QsU_x is
0086 91E3DB3A
32935960 8FD19C1B 79695C6E 0456DA8F BC9233C1 B35A6A4D

QsU_y is
0189 5D0FD0DB
3B7857DA 30AD06D5 66EA6175 AA71A5C3 17B35F4F A277150A

dsV is
0033 46FBC42B
1697AD26 931216B2 E8A5B891 B4637443 E20D6F42 23137E35

QsV_x is
001A 3B8CF983
8B02F471 A024FFEB E05D2A2B B5CE5E37 DDAC00AF 41317107

QsV_y is
009B C3C8E40D
E5E2F9CB 63A31985 1DB72F96 671503CC 45550230 6828347E

---
no Key Confirmation
NonceU is
004D 56F9346A
8B9C90B5 565EB261 F794D585 DB224A4C 3AB2C154 8CF1416D

Z is

                                                0041 38976F13
        E5F54BBD 2F24432B A5194E9B F737DF24 70F0B1CF 0440BF70

OtherInfo is
                                                12345678 9ABCDEF0
        414C4943 45313233 E900004D 56F9346A 8B9C90B5 565EB261
        F794D585 DB224A4C 3AB2C154 8CF1416D 424F4242 59343536

DerivedKeyMaterial is
                                                93109538 A048BC1E
        0EBCDEFD E3569A36 55775CCC C9EA6773 75E1C7F1 27D5CCA1
        B5617CC8 A59A9F85 2C019E1B F93EC1A0 76DDDA6B B3957812

KeyData is
                                                93109538 A048BC1E
        0EBCDEFD E3569A36 55775CCC C9EA6773 75E1C7F1 27D5CCA1
        B5617CC8 A59A9F85 2C019E1B F93EC1A0 76DDDA6B B3957812

Scheme Initiator, Key Confirmation Provider: U to V
NonceU is
                                                004D 56F9346A
        8B9C90B5 565EB261 F794D585 DB224A4C 3AB2C154 8CF1416D

NonceV is
                                                007B FD7AD6DD
        1621FB9A 169D413B 0B4E63A9 20A321B2 162971D8 D8E7464B

Z is
                                                0041 38976F13
        E5F54BBD 2F24432B A5194E9B F737DF24 70F0B1CF 0440BF70

OtherInfo is
                                                12345678 9ABCDEF0
        414C4943 45313233 E900004D 56F9346A 8B9C90B5 565EB261
        F794D585 DB224A4C 3AB2C154 8CF1416D 424F4242 59343536

```
DerivedKeyMaterial is
            9310 9538A048 BC1E0EBC DEFDE356 9A365577 5CCCC9EA
        677375E1 C7F127D5 CCA1B561 7CC8A59A 9F852C01 9E1BF93E
        C1A076DD DA6BB395 7812EB05 579EFAF3 24F0F73C FD17ABA9


MacData is
                                                        4B435F31
        5F55414C 49434542 4F424259 004D56F9 346A8B9C 90B5565E
        B261F794 D585DB22 4A4C3AB2 C1548CF1 416D007B FD7AD6DD
        1621FB9A 169D413B 0B4E63A9 20A321B2 162971D8 D8E7464B


MacKey is
                              9310 9538A048 BC1E0EBC DEFDE356


Mtag is
                                                        F550FB40
        04A5996E 74807169 D83E6486 AC78B2ED 478856A0 43068DA2


KeyData is
                                               9A365577 5CCCC9EA
        677375E1 C7F127D5 CCA1B561 7CC8A59A 9F852C01 9E1BF93E
        C1A076DD DA6BB395 7812EB05 579EFAF3 24F0F73C FD17ABA9




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceV is
                                                    007B FD7AD6DD
        1621FB9A 169D413B 0B4E63A9 20A321B2 162971D8 D8E7464B


NonceU is
                                                    004D 56F9346A
        8B9C90B5 565EB261 F794D585 DB224A4C 3AB2C154 8CF1416D


Z is
                                                    0041 38976F13
        E5F54BBD 2F24432B A5194E9B F737DF24 70F0B1CF 0440BF70
```

```
OtherInfo is
                                              12345678 9ABCDEF0
        414C4943 45313233 E900004D 56F9346A 8B9C90B5 565EB261
        F794D585 DB224A4C 3AB2C154 8CF1416D 424F4242 59343536


DerivedKeyMaterial is
            9310 9538A048 BC1E0EBC DEFDE356 9A365577 5CCCC9EA
        677375E1 C7F127D5 CCA1B561 7CC8A59A 9F852C01 9E1BF93E
        C1A076DD DA6BB395 7812EB05 579EFAF3 24F0F73C FD17ABA9


MacData is
            4B43 5F315F56 424F4242 59414C49 4345004D 56F9346A
        8B9C90B5 565EB261 F794D585 DB224A4C 3AB2C154 8CF1416D


MacKey is
                              9310 9538A048 BC1E0EBC DEFDE356


Mtag is
                                                      DB76E48E
        85D2E8F5 E247C8E7 A6BA2412 FCD1F6AE 056E4847 9E611C02


KeyData is
                                              9A365577 5CCCC9EA
        677375E1 C7F127D5 CCA1B561 7CC8A59A 9F852C01 9E1BF93E
        C1A076DD DA6BB395 7812EB05 579EFAF3 24F0F73C FD17ABA9




------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
NonceU is
                                                  004D 56F9346A
        8B9C90B5 565EB261 F794D585 DB224A4C 3AB2C154 8CF1416D


NonceV is
                                                  007B FD7AD6DD
```

```
        1621FB9A 169D413B 0B4E63A9 20A321B2 162971D8 D8E7464B


Z is
                                                    0041 38976F13
        E5F54BBD 2F24432B A5194E9B F737DF24 70F0B1CF 0440BF70


OtherInfo is
                                                12345678 9ABCDEF0
        414C4943 45313233 E900004D 56F9346A 8B9C90B5 565EB261
        F794D585 DB224A4C 3AB2C154 8CF1416D 424F4242 59343536


DerivedKeyMaterial is
            9310 9538A048 BC1E0EBC DEFDE356 9A365577 5CCCC9EA
        677375E1 C7F127D5 CCA1B561 7CC8A59A 9F852C01 9E1BF93E
        C1A076DD DA6BB395 7812EB05 579EFAF3 24F0F73C FD17ABA9


U2V
----------------
MacData is
                                                        4B435F32
        5F55414C 49434542 4F424259 004D56F9 346A8B9C 90B5565E
        B261F794 D585DB22 4A4C3AB2 C1548CF1 416D007B FD7AD6DD
        1621FB9A 169D413B 0B4E63A9 20A321B2 162971D8 D8E7464B


MacKey is
                                9310 9538A048 BC1E0EBC DEFDE356


Mtag is
                                                        533A2210
        B2F865F7 96345D47 29157A04 85994CB6 4F71721B F9BC1BE3


V2U
----------------
MacData is
                                                        4B435F32
        5F56424F 42425941 4C494345 007BFD7A D6DD1621 FB9A169D
        413B0B4E 63A920A3 21B21629 71D8D8E7 464B004D 56F9346A
        8B9C90B5 565EB261 F794D585 DB224A4C 3AB2C154 8CF1416D
```

MacKey is

9310 9538A048 BC1E0EBC DEFDE356

Mtag is

47F995E9
92E3A225 AB9476B9 00BE61DF 179CCDD9 CAE7746C E3348896

KeyData is

9A365577 5CCCC9EA
677375E1 C7F127D5 CCA1B561 7CC8A59A 9F852C01 9E1BF93E
C1A076DD DA6BB395 7812EB05 579EFAF3 24F0F73C FD17ABA9

FullUnifiedCDH(B-233)
---
dsU is
0028 C281947E
8AD75CE7 7A7B01A4 89EF119E 73A0AF5A 61CC6416 0538E006

QsU_x is
014E 6A55284E
9E45672D 62DA3226 E1A3F816 ABA63013 0DAA641C 8251B1B1

QsU_y is
01D6 D3886B22
76FEC7D4 E2E629DA CA836A8B B0DAA6DF C3A7F86C 92774500

dsV is
009F 15263D98
EFEAB4FB 391C1266 350E6E78 00F17F3C 93B1FF64 845D5AB6

QsV_x is
00FD 20CE00C9
FD550D7D 9B4731D3 7FD7F52E 7A723F98 6424E7B8 B1372200

QsV_y is
01E2 442FACB3
1097ACD7 CEC15415 7352CFD2 DB240AD3 18B1116D 7A6FEBA0

deU is
00C9 199D23BB
CEBE9E61 8F7423DD 6466DA30 70CE38C8 EE46424F 3565916D

QeU_x is
0197 0E7CFD98
C2010742 A0E369C4 03F5D705 3CD18AB4 790DE1D8 E3A5CDE2

QeU_y is
013A EEC85FE6

```
        FFC7DBC7 EE28AEE6 B9EFF2DA D6F8858E 4B938D34 6C8880DD


deV is
                                                    0013 7D9E5F48
        2950E6F9 7738DF43 20DA1CFE 9B121430 5C2CE1AF EE7AC5F5


QeV_x is
                                                    01FF A7168582
        30FEAC12 34F0888A 55CA0A33 FF3C86F0 6F2AC93F A31CF885


QeV_y is
                                                    0011 97EAB0FF
        51B4A302 467EA3FC E6F35F21 D4668F92 66ED4EE1 F7E814E3




------------------------------------------------------------
no Key Confirmation
Zs is
                                                    00C5 FF53E4B5
        5E87A22C 6F85453A AF6D9DDB 508E7ABA 61E253BC 359B6253


Ze is
                                                    01BA CB50D15F
        D8EC1FA2 BECD8F02 B15D5CCD E5BD133F 1703D0CF D99BB9F6


Z is
                                    01BACB50 D15FD8EC 1FA2BECD
        8F02B15D 5CCDE5BD 133F1703 D0CFD99B B9F600C5 FF53E4B5
        5E87A22C 6F85453A AF6D9DDB 508E7ABA 61E253BC 359B6253


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                    88059C03 1EB58727
        8D3CE770 6071E360 93BC60A1 3CFDCF0B A3186B14 94938559
        8C1B8E58 2E85C98A 00E8461A 2982A4CA 58442E4C FFF49F62
```

KeyData is
                                                88059C03 1EB58727
        8D3CE770 6071E360 93BC60A1 3CFDCF0B A3186B14 94938559
        8C1B8E58 2E85C98A 00E8461A 2982A4CA 58442E4C FFF49F62

Scheme Initiator, Key Confirmation Provider: U to V
Zs is
                                                    00C5 FF53E4B5
        5E87A22C 6F85453A AF6D9DDB 508E7ABA 61E253BC 359B6253

Ze is
                                                    01BA CB50D15F
        D8EC1FA2 BECD8F02 B15D5CCD E5BD133F 1703D0CF D99BB9F6

Z is
                                    01BACB50 D15FD8EC 1FA2BECD
        8F02B15D 5CCDE5BD 133F1703 D0CFD99B B9F600C5 FF53E4B5
        5E87A22C 6F85453A AF6D9DDB 508E7ABA 61E253BC 359B6253

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
            8805 9C031EB5 87278D3C E7706071 E36093BC 60A13CFD
        CF0BA318 6B149493 85598C1B 8E582E85 C98A00E8 461A2982
        A4CA5844 2E4CFFF4 9F6207CE 00F3CFE5 93695352 17217597

MacData is
                          4B435F31 5F55414C 49434542 4F424259
        01970E7C FD98C201 0742A0E3 69C403F5 D7053CD1 8AB4790D
        E1D8E3A5 CDE2013A EEC85FE6 FFC7DBC7 EE28AEE6 B9EFF2DA
        D6F8858E 4B938D34 6C8880DD 01FFA716 858230FE AC1234F0
        888A55CA 0A33FF3C 86F06F2A C93FA31C F8850011 97EAB0FF
        51B4A302 467EA3FC E6F35F21 D4668F92 66ED4EE1 F7E814E3

MacKey is
                              8805 9C031EB5 87278D3C E7706071

Mtag is
                                                      698C4BD7
        079AFA18 0BA53ED8 1637F90E 4412BF89 4BC3A426 ABDCF29E

KeyData is
                                             E36093BC 60A13CFD
        CF0BA318 6B149493 85598C1B 8E582E85 C98A00E8 461A2982
        A4CA5844 2E4CFFF4 9F6207CE 00F3CFE5 93695352 17217597

Scheme Responder, Key Confirmation Provider: V to U
Zs is
                                                 00C5 FF53E4B5
        5E87A22C 6F85453A AF6D9DDB 508E7ABA 61E253BC 359B6253

Ze is
                                                 01BA CB50D15F
        D8EC1FA2 BECD8F02 B15D5CCD E5BD133F 1703D0CF D99BB9F6

Z is
                                    01BACB50 D15FD8EC 1FA2BECD
        8F02B15D 5CCDE5BD 133F1703 D0CFD99B B9F600C5 FF53E4B5
        5E87A22C 6F85453A AF6D9DDB 508E7ABA 61E253BC 359B6253

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
            8805 9C031EB5 87278D3C E7706071 E36093BC 60A13CFD
        CF0BA318 6B149493 85598C1B 8E582E85 C98A00E8 461A2982
        A4CA5844 2E4CFFF4 9F6207CE 00F3CFE5 93695352 17217597

```
MacData is
                          4B435F31 5F56424F 42425941 4C494345
        01FFA716 858230FE AC1234F0 888A55CA 0A33FF3C 86F06F2A
        C93FA31C F8850011 97EAB0FF 51B4A302 467EA3FC E6F35F21
        D4668F92 66ED4EE1 F7E814E3 01970E7C FD98C201 0742A0E3
        69C403F5 D7053CD1 8AB4790D E1D8E3A5 CDE2013A EEC85FE6
        FFC7DBC7 EE28AEE6 B9EFF2DA D6F8858E 4B938D34 6C8880DD


MacKey is
                               8805 9C031EB5 87278D3C E7706071


Mtag is
                                                        8BE338DE
        76567201 28593F0B 01AD5AD3 FCBA2280 88FCB5C0 3185B099


KeyData is
                                                E36093BC 60A13CFD
        CF0BA318 6B149493 85598C1B 8E582E85 C98A00E8 461A2982
        A4CA5844 2E4CFFF4 9F6207CE 00F3CFE5 93695352 17217597




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
Zs is
                                                    00C5 FF53E4B5
        5E87A22C 6F85453A AF6D9DDB 508E7ABA 61E253BC 359B6253


Ze is
                                                    01BA CB50D15F
        D8EC1FA2 BECD8F02 B15D5CCD E5BD133F 1703D0CF D99BB9F6


Z is
                                   01BACB50 D15FD8EC 1FA2BECD
        8F02B15D 5CCDE5BD 133F1703 D0CFD99B B9F600C5 FF53E4B5
        5E87A22C 6F85453A AF6D9DDB 508E7ABA 61E253BC 359B6253


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536
```

```
DerivedKeyMaterial is
            8805 9C031EB5 87278D3C E7706071 E36093BC 60A13CFD
        CF0BA318 6B149493 85598C1B 8E582E85 C98A00E8 461A2982
        A4CA5844 2E4CFFF4 9F6207CE 00F3CFE5 93695352 17217597


U2V
----------------
MacData is
                         4B435F32 5F55414C 49434542 4F424259
        01970E7C FD98C201 0742A0E3 69C403F5 D7053CD1 8AB4790D
        E1D8E3A5 CDE2013A EEC85FE6 FFC7DBC7 EE28AEE6 B9EFF2DA
        D6F8858E 4B938D34 6C8880DD 01FFA716 858230FE AC1234F0
        888A55CA 0A33FF3C 86F06F2A C93FA31C F8850011 97EAB0FF
        51B4A302 467EA3FC E6F35F21 D4668F92 66ED4EE1 F7E814E3


MacKey is
                              8805 9C031EB5 87278D3C E7706071


Mtag is
                                                        91A91560
        E105CE5B 7096FC3B EC9A2F9A B4C4744E 8F3FDD94 6B1F3E7D


V2U
----------------
MacData is
                         4B435F32 5F56424F 42425941 4C494345
        01FFA716 858230FE AC1234F0 888A55CA 0A33FF3C 86F06F2A
        C93FA31C F8850011 97EAB0FF 51B4A302 467EA3FC E6F35F21
        D4668F92 66ED4EE1 F7E814E3 01970E7C FD98C201 0742A0E3
        69C403F5 D7053CD1 8AB4790D E1D8E3A5 CDE2013A EEC85FE6
        FFC7DBC7 EE28AEE6 B9EFF2DA D6F8858E 4B938D34 6C8880DD


MacKey is
                              8805 9C031EB5 87278D3C E7706071


Mtag is
                                                        0064C880
        4F66D35C 58E450D4 4008A791 B7E39567 4527A4AD 36E97006
```

KeyData is
                                                E36093BC 60A13CFD
        CF0BA318 6B149493 85598C1B 8E582E85 C98A00E8 461A2982
        A4CA5844 2E4CFFF4 9F6207CE 00F3CFE5 93695352 17217597

FullMQV(B-233)
----
dsU is
                                                    0028 C281947E
        8AD75CE7 7A7B01A4 89EF119E 73A0AF5A 61CC6416 0538E006

QsU_x is
                                                    014E 6A55284E
        9E45672D 62DA3226 E1A3F816 ABA63013 0DAA641C 8251B1B1

QsU_y is
                                                    01D6 D3886B22
        76FEC7D4 E2E629DA CA836A8B B0DAA6DF C3A7F86C 92774500

dsV is
                                                    009F 15263D98
        EFEAB4FB 391C1266 350E6E78 00F17F3C 93B1FF64 845D5AB6

QsV_x is
                                                    00FD 20CE00C9
        FD550D7D 9B4731D3 7FD7F52E 7A723F98 6424E7B8 B1372200

QsV_y is
                                                    01E2 442FACB3
        1097ACD7 CEC15415 7352CFD2 DB240AD3 18B1116D 7A6FEBA0

deU is
                                                    00C9 199D23BB
        CEBE9E61 8F7423DD 6466DA30 70CE38C8 EE46424F 3565916D

```
QeU_x is
                                                  0197 0E7CFD98
        C2010742 A0E369C4 03F5D705 3CD18AB4 790DE1D8 E3A5CDE2


QeU_y is
                                                  013A EEC85FE6
        FFC7DBC7 EE28AEE6 B9EFF2DA D6F8858E 4B938D34 6C8880DD


deV is
                                                  0013 7D9E5F48
        2950E6F9 7738DF43 20DA1CFE 9B121430 5C2CE1AF EE7AC5F5


QeV_x is
                                                  01FF A7168582
        30FEAC12 34F0888A 55CA0A33 FF3C86F0 6F2AC93F A31CF885


QeV_y is
                                                  0011 97EAB0FF
        51B4A302 467EA3FC E6F35F21 D4668F92 66ED4EE1 F7E814E3




------------------------------------------------------------
no Key Confirmation
Z is
                                                  0063 F8674931
        93B38209 6CBD106F 7AA869B8 5EAC2E4C 22CA1A1C 2C93EF0B


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                  97E7CC4C EFE9D2B4
        3E21C7A7 5B843C24 B09E832C 47AB69E7 8AD47556 A78950B6
        77245E42 00EDB57E 1B689671 1E838B43 68EC1B45 842084D0


KeyData is
```

                                                97E7CC4C EFE9D2B4
        3E21C7A7 5B843C24 B09E832C 47AB69E7 8AD47556 A78950B6
        77245E42 00EDB57E 1B689671 1E838B43 68EC1B45 842084D0

Scheme Initiator, Key Confirmation Provider: U to V
Z is
                                                    0063 F8674931
        93B38209 6CBD106F 7AA869B8 5EAC2E4C 22CA1A1C 2C93EF0B

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
            97E7 CC4CEFE9 D2B43E21 C7A75B84 3C24B09E 832C47AB
        69E78AD4 7556A789 50B67724 5E4200ED B57E1B68 96711E83
        8B4368EC 1B458420 84D09FBA 9846DA96 E4CA64BB A47F6237

MacData is
                          4B435F31 5F55414C 49434542 4F424259
        01970E7C FD98C201 0742A0E3 69C403F5 D7053CD1 8AB4790D
        E1D8E3A5 CDE2013A EEC85FE6 FFC7DBC7 EE28AEE6 B9EFF2DA
        D6F8858E 4B938D34 6C8880DD 01FFA716 858230FE AC1234F0
        888A55CA 0A33FF3C 86F06F2A C93FA31C F8850011 97EAB0FF
        51B4A302 467EA3FC E6F35F21 D4668F92 66ED4EE1 F7E814E3

MacKey is
                               97E7 CC4CEFE9 D2B43E21 C7A75B84

Mtag is
                                                        5408634C
        022B58D2 6C4906F4 20FDA682 9E8CD2F8 8DCD2C6D A8970106

KeyData is
                                                    3C24B09E 832C47AB
        69E78AD4 7556A789 50B67724 5E4200ED B57E1B68 96711E83
        8B4368EC 1B458420 84D09FBA 9846DA96 E4CA64BB A47F6237

```
-------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
                                                  0063 F8674931
        93B38209 6CBD106F 7AA869B8 5EAC2E4C 22CA1A1C 2C93EF0B


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            97E7 CC4CEFE9 D2B43E21 C7A75B84 3C24B09E 832C47AB
        69E78AD4 7556A789 50B67724 5E4200ED B57E1B68 96711E83
        8B4368EC 1B458420 84D09FBA 9846DA96 E4CA64BB A47F6237


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        01FFA716 858230FE AC1234F0 888A55CA 0A33FF3C 86F06F2A
        C93FA31C F8850011 97EAB0FF 51B4A302 467EA3FC E6F35F21
        D4668F92 66ED4EE1 F7E814E3 01970E7C FD98C201 0742A0E3
        69C403F5 D7053CD1 8AB4790D E1D8E3A5 CDE2013A EEC85FE6
        FFC7DBC7 EE28AEE6 B9EFF2DA D6F8858E 4B938D34 6C8880DD


MacKey is
                             97E7 CC4CEFE9 D2B43E21 C7A75B84


Mtag is
                                                      A523B39F
        3C2724CC B666D629 D5860500 876B6980 F9D1FBAF 3C2F31DD


KeyData is
                                                  3C24B09E 832C47AB
        69E78AD4 7556A789 50B67724 5E4200ED B57E1B68 96711E83
        8B4368EC 1B458420 84D09FBA 9846DA96 E4CA64BB A47F6237
```

```
------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
Z is
                                                    0063 F8674931
        93B38209 6CBD106F 7AA869B8 5EAC2E4C 22CA1A1C 2C93EF0B


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            97E7 CC4CEFE9 D2B43E21 C7A75B84 3C24B09E 832C47AB
        69E78AD4 7556A789 50B67724 5E4200ED B57E1B68 96711E83
        8B4368EC 1B458420 84D09FBA 9846DA96 E4CA64BB A47F6237


U2V
----------------
MacData is
                         4B435F32 5F55414C 49434542 4F424259
        01970E7C FD98C201 0742A0E3 69C403F5 D7053CD1 8AB4790D
        E1D8E3A5 CDE2013A EEC85FE6 FFC7DBC7 EE28AEE6 B9EFF2DA
        D6F8858E 4B938D34 6C8880DD 01FFA716 858230FE AC1234F0
        888A55CA 0A33FF3C 86F06F2A C93FA31C F8850011 97EAB0FF
        51B4A302 467EA3FC E6F35F21 D4668F92 66ED4EE1 F7E814E3


MacKey is
                             97E7 CC4CEFE9 D2B43E21 C7A75B84


Mtag is
                                                        CF9C3E3A
        0C418A8C 8D852B22 A0632BD6 20426A86 6D5861BD 5D505F7D


V2U
----------------
MacData is
                         4B435F32 5F56424F 42425941 4C494345
        01FFA716 858230FE AC1234F0 888A55CA 0A33FF3C 86F06F2A
        C93FA31C F8850011 97EAB0FF 51B4A302 467EA3FC E6F35F21
        D4668F92 66ED4EE1 F7E814E3 01970E7C FD98C201 0742A0E3
```

```
        69C403F5 D7053CD1 8AB4790D E1D8E3A5 CDE2013A EEC85FE6
        FFC7DBC7 EE28AEE6 B9EFF2DA D6F8858E 4B938D34 6C8880DD


MacKey is
                            97E7 CC4CEFE9 D2B43E21 C7A75B84


Mtag is
                                                    184BEB34
        0DC2C13E 3E73F839 3416B417 58B5A363 2ADE82DD B1777E9A


KeyData is
                                               3C24B09E 832C47AB
        69E78AD4 7556A789 50B67724 5E4200ED B57E1B68 96711E83
        8B4368EC 1B458420 84D09FBA 9846DA96 E4CA64BB A47F6237




EphemeralUnifiedCDH(B-233)
-----------------------------------------------------------
deU is
                                                   00C9 199D23BB
        CEBE9E61 8F7423DD 6466DA30 70CE38C8 EE46424F 3565916D


QeU_x is
                                                   0197 0E7CFD98
        C2010742 A0E369C4 03F5D705 3CD18AB4 790DE1D8 E3A5CDE2


QeU_y is
                                                   013A EEC85FE6
        FFC7DBC7 EE28AEE6 B9EFF2DA D6F8858E 4B938D34 6C8880DD


deV is
                                                   0013 7D9E5F48
        2950E6F9 7738DF43 20DA1CFE 9B121430 5C2CE1AF EE7AC5F5


QeV_x is
                                                   01FF A7168582
        30FEAC12 34F0888A 55CA0A33 FF3C86F0 6F2AC93F A31CF885
```

```
QeV_y is
                                                  0011 97EAB0FF
        51B4A302 467EA3FC E6F35F21 D4668F92 66ED4EE1 F7E814E3



------------------------------------------------------------
no Key Confirmation
Z is
                                                  01BA CB50D15F
        D8EC1FA2 BECD8F02 B15D5CCD E5BD133F 1703D0CF D99BB9F6


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                  8ED9113E 432E09FD
        76C5C550 B39DE967 F03C3D1B 7EB08F01 F5011143 0A267D61
        108A8829 9D6627B3 1F5AD1BC E82078BD 43410E9B C9C8617F


KeyData is
                                                  8ED9113E 432E09FD
        76C5C550 B39DE967 F03C3D1B 7EB08F01 F5011143 0A267D61
        108A8829 9D6627B3 1F5AD1BC E82078BD 43410E9B C9C8617F



OnePassUnifiedCDH(B-233)
------------------------------------------------------------
dsU is
                                                  0028 C281947E
        8AD75CE7 7A7B01A4 89EF119E 73A0AF5A 61CC6416 0538E006


QsU_x is
                                                  014E 6A55284E
        9E45672D 62DA3226 E1A3F816 ABA63013 0DAA641C 8251B1B1
```

```
QsU_y is
                                                    01D6 D3886B22
        76FEC7D4 E2E629DA CA836A8B B0DAA6DF C3A7F86C 92774500


dsV is
                                                    009F 15263D98
        EFEAB4FB 391C1266 350E6E78 00F17F3C 93B1FF64 845D5AB6


QsV_x is
                                                    00FD 20CE00C9
        FD550D7D 9B4731D3 7FD7F52E 7A723F98 6424E7B8 B1372200


QsV_y is
                                                    01E2 442FACB3
        1097ACD7 CEC15415 7352CFD2 DB240AD3 18B1116D 7A6FEBA0


deU is
                                                    00C9 199D23BB
        CEBE9E61 8F7423DD 6466DA30 70CE38C8 EE46424F 3565916D


QeU_x is
                                                    0197 0E7CFD98
        C2010742 A0E369C4 03F5D705 3CD18AB4 790DE1D8 E3A5CDE2


QeU_y is
                                                    013A EEC85FE6
        FFC7DBC7 EE28AEE6 B9EFF2DA D6F8858E 4B938D34 6C8880DD




------------------------------------------------------------
no Key Confirmation
Zs is
                                                    00C5 FF53E4B5
        5E87A22C 6F85453A AF6D9DDB 508E7ABA 61E253BC 359B6253


Ze is
                                                    00D9 EDA652A1
```

```
        B31A4CF7 015C6B2B B0930A9F 83ADDCB9 832EA904 5B5D326B


Z is
                                    00D9EDA6 52A1B31A 4CF7015C
        6B2BB093 0A9F83AD DCB9832E A9045B5D 326B00C5 FF53E4B5
        5E87A22C 6F85453A AF6D9DDB 508E7ABA 61E253BC 359B6253


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                80431140 E7C20FB1
        92F1574A 31197260 5F8EBEBF F607025C D423891D 73EA6F72
        3FDE638D 22A168D7 69EE9922 EFCE8EF8 FB4A7F25 789A9E12


KeyData is
                                                80431140 E7C20FB1
        92F1574A 31197260 5F8EBEBF F607025C D423891D 73EA6F72
        3FDE638D 22A168D7 69EE9922 EFCE8EF8 FB4A7F25 789A9E12




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                                                    00AC F775AE0C
        2C707136 0C88D1F3 857D0799 9BD90663 131F3F6E 4190928F


Zs is
                                                    00C5 FF53E4B5
        5E87A22C 6F85453A AF6D9DDB 508E7ABA 61E253BC 359B6253


Ze is
                                                    00D9 EDA652A1
        B31A4CF7 015C6B2B B0930A9F 83ADDCB9 832EA904 5B5D326B


Z is
                                    00D9EDA6 52A1B31A 4CF7015C
```

```
        6B2BB093 0A9F83AD DCB9832E A9045B5D 326B00C5 FF53E4B5
        5E87A22C 6F85453A AF6D9DDB 508E7ABA 61E253BC 359B6253


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            8043 1140E7C2 0FB192F1 574A3119 72605F8E BEBFF607
        025CD423 891D73EA 6F723FDE 638D22A1 68D769EE 9922EFCE
        8EF8FB4A 7F25789A 9E12E045 29A6BAF3 B6306BDC B0D34B49


MacData is
                                       4B43 5F315F55 414C4943
        45424F42 42590197 0E7CFD98 C2010742 A0E369C4 03F5D705
        3CD18AB4 790DE1D8 E3A5CDE2 013AEEC8 5FE6FFC7 DBC7EE28
        AEE6B9EF F2DAD6F8 858E4B93 8D346C88 80DD00AC F775AE0C
        2C707136 0C88D1F3 857D0799 9BD90663 131F3F6E 4190928F


MacKey is
                               8043 1140E7C2 0FB192F1 574A3119


Mtag is
                                                       010ABABA
        7268575F 08CA2942 FC37F77C 3AC2AE20 647237F1 FDD76A40


KeyData is
                                              72605F8E BEBFF607
        025CD423 891D73EA 6F723FDE 638D22A1 68D769EE 9922EFCE
        8EF8FB4A 7F25789A 9E12E045 29A6BAF3 B6306BDC B0D34B49




-----------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
                                                   00AC F775AE0C
        2C707136 0C88D1F3 857D0799 9BD90663 131F3F6E 4190928F
```

```
Zs is
                                                  00C5 FF53E4B5
        5E87A22C 6F85453A AF6D9DDB 508E7ABA 61E253BC 359B6253


Ze is
                                                  00D9 EDA652A1
        B31A4CF7 015C6B2B B0930A9F 83ADDCB9 832EA904 5B5D326B


Z is
                                  00D9EDA6 52A1B31A 4CF7015C
        6B2BB093 0A9F83AD DCB9832E A9045B5D 326B00C5 FF53E4B5
        5E87A22C 6F85453A AF6D9DDB 508E7ABA 61E253BC 359B6253


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            8043 1140E7C2 0FB192F1 574A3119 72605F8E BEBFF607
        025CD423 891D73EA 6F723FDE 638D22A1 68D769EE 9922EFCE
        8EF8FB4A 7F25789A 9E12E045 29A6BAF3 B6306BDC B0D34B49


MacData is
                                                    4B435F31
        5F56424F 42425941 4C494345 01970E7C FD98C201 0742A0E3
        69C403F5 D7053CD1 8AB4790D E1D8E3A5 CDE2013A EEC85FE6
        FFC7DBC7 EE28AEE6 B9EFF2DA D6F8858E 4B938D34 6C8880DD


MacKey is
                             8043 1140E7C2 0FB192F1 574A3119


Mtag is
                                                    7CDA448A
        3DD7FF37 9C155911 48A25B86 07BE80AA A05E6BCB 1F6EC479


KeyData is
                                                  72605F8E BEBFF607
        025CD423 891D73EA 6F723FDE 638D22A1 68D769EE 9922EFCE
        8EF8FB4A 7F25789A 9E12E045 29A6BAF3 B6306BDC B0D34B49
```

```
-------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
                                                    00AC F775AE0C
        2C707136 0C88D1F3 857D0799 9BD90663 131F3F6E 4190928F


Zs is
                                                    00C5 FF53E4B5
        5E87A22C 6F85453A AF6D9DDB 508E7ABA 61E253BC 359B6253


Ze is
                                                    00D9 EDA652A1
        B31A4CF7 015C6B2B B0930A9F 83ADDCB9 832EA904 5B5D326B


Z is
                                    00D9EDA6 52A1B31A 4CF7015C
        6B2BB093 0A9F83AD DCB9832E A9045B5D 326B00C5 FF53E4B5
        5E87A22C 6F85453A AF6D9DDB 508E7ABA 61E253BC 359B6253


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            8043 1140E7C2 0FB192F1 574A3119 72605F8E BEBFF607
        025CD423 891D73EA 6F723FDE 638D22A1 68D769EE 9922EFCE
        8EF8FB4A 7F25789A 9E12E045 29A6BAF3 B6306BDC B0D34B49


U2V
----------------
MacData is
                                        4B43 5F325F55 414C4943
        45424F42 42590197 0E7CFD98 C2010742 A0E369C4 03F5D705
        3CD18AB4 790DE1D8 E3A5CDE2 013AEEC8 5FE6FFC7 DBC7EE28
        AEE6B9EF F2DAD6F8 858E4B93 8D346C88 80DD00AC F775AE0C
        2C707136 0C88D1F3 857D0799 9BD90663 131F3F6E 4190928F
```

```
MacKey is
                              8043 1140E7C2 0FB192F1 574A3119


Mtag is
                                                        23599831
        C3AAC6A3 4A3B363A 5CF2F3CC 5F5B8D42 918BDB14 8B2FE26B


V2U
----------------
MacData is
                                       4B43 5F325F56 424F4242
        59414C49 434500AC F775AE0C 2C707136 0C88D1F3 857D0799
        9BD90663 131F3F6E 4190928F 01970E7C FD98C201 0742A0E3
        69C403F5 D7053CD1 8AB4790D E1D8E3A5 CDE2013A EEC85FE6
        FFC7DBC7 EE28AEE6 B9EFF2DA D6F8858E 4B938D34 6C8880DD


MacKey is
                              8043 1140E7C2 0FB192F1 574A3119


Mtag is
                                                        72DFBA8F
        8160356F 4ACA7BED A83266AF D5BA53A2 CE319DD6 9827D8EA


KeyData is
                                               72605F8E BEBFF607
        025CD423 891D73EA 6F723FDE 638D22A1 68D769EE 9922EFCE
        8EF8FB4A 7F25789A 9E12E045 29A6BAF3 B6306BDC B0D34B49




OnePassMQV(B-233)
------------------------------------------------------------
dsU is
                                                    0028 C281947E
        8AD75CE7 7A7B01A4 89EF119E 73A0AF5A 61CC6416 0538E006


QsU_x is
                                                    014E 6A55284E
```

9E45672D 62DA3226 E1A3F816 ABA63013 0DAA641C 8251B1B1

QsU_y is
01D6 D3886B22
76FEC7D4 E2E629DA CA836A8B B0DAA6DF C3A7F86C 92774500

dsV is
009F 15263D98
EFEAB4FB 391C1266 350E6E78 00F17F3C 93B1FF64 845D5AB6

QsV_x is
00FD 20CE00C9
FD550D7D 9B4731D3 7FD7F52E 7A723F98 6424E7B8 B1372200

QsV_y is
01E2 442FACB3
1097ACD7 CEC15415 7352CFD2 DB240AD3 18B1116D 7A6FEBA0

deU is
00C9 199D23BB
CEBE9E61 8F7423DD 6466DA30 70CE38C8 EE46424F 3565916D

QeU_x is
0197 0E7CFD98
C2010742 A0E369C4 03F5D705 3CD18AB4 790DE1D8 E3A5CDE2

QeU_y is
013A EEC85FE6
FFC7DBC7 EE28AEE6 B9EFF2DA D6F8858E 4B938D34 6C8880DD

---
no Key Confirmation
Z is
005D D81A23A9
2337BA31 C5A6A807 B9AB2052 0E3A66B9 4353DE9E FD3D4056

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                00787F92 A32942CD
        8702ED25 68A4C959 C47F2B93 4D1C8662 37487361 369DFD48
        45A4FD0D 8A191EF4 974CEBF9 8102ADFA 741C5149 403A30EC


KeyData is
                                                00787F92 A32942CD
        8702ED25 68A4C959 C47F2B93 4D1C8662 37487361 369DFD48
        45A4FD0D 8A191EF4 974CEBF9 8102ADFA 741C5149 403A30EC




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                                                    00AC F775AE0C
        2C707136 0C88D1F3 857D0799 9BD90663 131F3F6E 4190928F


Z is
                                                    005D D81A23A9
        2337BA31 C5A6A807 B9AB2052 0E3A66B9 4353DE9E FD3D4056


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            0078 7F92A329 42CD8702 ED2568A4 C959C47F 2B934D1C
        86623748 7361369D FD4845A4 FD0D8A19 1EF4974C EBF98102
        ADFA741C 5149403A 30ECD552 78E0AEB2 553DC298 52E75157


MacData is
                                        4B43 5F315F55 414C4943
        45424F42 42590197 0E7CFD98 C2010742 A0E369C4 03F5D705
        3CD18AB4 790DE1D8 E3A5CDE2 013AEEC8 5FE6FFC7 DBC7EE28
        AEE6B9EF F2DAD6F8 858E4B93 8D346C88 80DD00AC F775AE0C
```

```
        2C707136 0C88D1F3 857D0799 9BD90663 131F3F6E 4190928F


MacKey is
                              0078 7F92A329 42CD8702 ED2568A4


Mtag is
                                                        485AC3D7
        5E14A398 8224EABC 94BBD812 930F2DC9 BFF8FF8B CAF375FF


KeyData is
                                                C959C47F 2B934D1C
        86623748 7361369D FD4845A4 FD0D8A19 1EF4974C EBF98102
        ADFA741C 5149403A 30ECD552 78E0AEB2 553DC298 52E75157




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
                                                    00AC F775AE0C
        2C707136 0C88D1F3 857D0799 9BD90663 131F3F6E 4190928F


Z is
                                                    005D D81A23A9
        2337BA31 C5A6A807 B9AB2052 0E3A66B9 4353DE9E FD3D4056


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            0078 7F92A329 42CD8702 ED2568A4 C959C47F 2B934D1C
        86623748 7361369D FD4845A4 FD0D8A19 1EF4974C EBF98102
        ADFA741C 5149403A 30ECD552 78E0AEB2 553DC298 52E75157


MacData is
                                                        4B435F31
        5F56424F 42425941 4C494345 01970E7C FD98C201 0742A0E3
        69C403F5 D7053CD1 8AB4790D E1D8E3A5 CDE2013A EEC85FE6
```

```
        FFC7DBC7 EE28AEE6 B9EFF2DA D6F8858E 4B938D34 6C8880DD


MacKey is
                              0078 7F92A329 42CD8702 ED2568A4


Mtag is
                                                      8E841C44
        FF8CB9C5 096895A2 864E22FE 77DE82AA 364F3046 ADE68F14


KeyData is
                                                 C959C47F 2B934D1C
        86623748 7361369D FD4845A4 FD0D8A19 1EF4974C EBF98102
        ADFA741C 5149403A 30ECD552 78E0AEB2 553DC298 52E75157




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
                                                    00AC F775AE0C
        2C707136 0C88D1F3 857D0799 9BD90663 131F3F6E 4190928F


Z is
                                                    005D D81A23A9
        2337BA31 C5A6A807 B9AB2052 0E3A66B9 4353DE9E FD3D4056


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            0078 7F92A329 42CD8702 ED2568A4 C959C47F 2B934D1C
        86623748 7361369D FD4845A4 FD0D8A19 1EF4974C EBF98102
        ADFA741C 5149403A 30ECD552 78E0AEB2 553DC298 52E75157


U2V
----------------
MacData is
                                       4B43 5F325F55 414C4943
```

```
        45424F42 42590197 0E7CFD98 C2010742 A0E369C4 03F5D705
        3CD18AB4 790DE1D8 E3A5CDE2 013AEEC8 5FE6FFC7 DBC7EE28
        AEE6B9EF F2DAD6F8 858E4B93 8D346C88 80DD00AC F775AE0C
        2C707136 0C88D1F3 857D0799 9BD90663 131F3F6E 4190928F


MacKey is
                            0078 7F92A329 42CD8702 ED2568A4


Mtag is
                                                    BB0C1A04
        06CE6F3C 7B2548FD 9CDCDA16 34879391 FA12D56C 78A5D8C6


V2U
----------------
MacData is
                                       4B43 5F325F56 424F4242
        59414C49 434500AC F775AE0C 2C707136 0C88D1F3 857D0799
        9BD90663 131F3F6E 4190928F 01970E7C FD98C201 0742A0E3
        69C403F5 D7053CD1 8AB4790D E1D8E3A5 CDE2013A EEC85FE6
        FFC7DBC7 EE28AEE6 B9EFF2DA D6F8858E 4B938D34 6C8880DD


MacKey is
                            0078 7F92A329 42CD8702 ED2568A4


Mtag is
                                                    C8795E94
        A9509D7E A572010B D3CFD282 2EA70D28 9B78CE80 1B1CE769


KeyData is
                                                C959C47F 2B934D1C
        86623748 7361369D FD4845A4 FD0D8A19 1EF4974C EBF98102
        ADFA741C 5149403A 30ECD552 78E0AEB2 553DC298 52E75157




OnePassDiffieHellmanCDH(B-233)
------------------------------------------------------------
dsV is
                                                    009F 15263D98
```

```
        EFEAB4FB 391C1266 350E6E78 00F17F3C 93B1FF64 845D5AB6


QsV_x is
                                                    00FD 20CE00C9
        FD550D7D 9B4731D3 7FD7F52E 7A723F98 6424E7B8 B1372200


QsV_y is
                                                    01E2 442FACB3
        1097ACD7 CEC15415 7352CFD2 DB240AD3 18B1116D 7A6FEBA0


deU is
                                                    00C9 199D23BB
        CEBE9E61 8F7423DD 6466DA30 70CE38C8 EE46424F 3565916D


QeU_x is
                                                    0197 0E7CFD98
        C2010742 A0E369C4 03F5D705 3CD18AB4 790DE1D8 E3A5CDE2


QeU_y is
                                                    013A EEC85FE6
        FFC7DBC7 EE28AEE6 B9EFF2DA D6F8858E 4B938D34 6C8880DD




------------------------------------------------------------
no Key Confirmation
Z is
                                                    00D9 EDA652A1
        B31A4CF7 015C6B2B B0930A9F 83ADDCB9 832EA904 5B5D326B


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                8DEF4EBA 38DFED3C
        6FCB72F4 8EE17B57 7F5B56EA C5EE32F2 69D78599 6C373E74
        B9E4A2F2 5A0F6B18 35F791A3 D4143EFC F77C66A6 64718CAD
```

KeyData is
                                                8DEF4EBA 38DFED3C
        6FCB72F4 8EE17B57 7F5B56EA C5EE32F2 69D78599 6C373E74
        B9E4A2F2 5A0F6B18 35F791A3 D4143EFC F77C66A6 64718CAD

Scheme Responder, Key Confirmation Provider: V to U
Z is
                                                    00D9 EDA652A1
        B31A4CF7 015C6B2B B0930A9F 83ADDCB9 832EA904 5B5D326B

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
            8DEF 4EBA38DF ED3C6FCB 72F48EE1 7B577F5B 56EAC5EE
        32F269D7 85996C37 3E74B9E4 A2F25A0F 6B1835F7 91A3D414
        3EFCF77C 66A66471 8CAD0F12 6AB0858D 022158B3 EF9B5046

MacData is
                                                        4B435F31
        5F56424F 42425941 4C494345 01970E7C FD98C201 0742A0E3
        69C403F5 D7053CD1 8AB4790D E1D8E3A5 CDE2013A EEC85FE6
        FFC7DBC7 EE28AEE6 B9EFF2DA D6F8858E 4B938D34 6C8880DD

MacKey is
                              8DEF 4EBA38DF ED3C6FCB 72F48EE1

Mtag is
                                                        DA3CF2AA
        7E2EA276 4582EBBC 9819DA2E 3A68EDD6 93E3E552 8351C7B6

KeyData is
                                                7B577F5B 56EAC5EE
        32F269D7 85996C37 3E74B9E4 A2F25A0F 6B1835F7 91A3D414
        3EFCF77C 66A66471 8CAD0F12 6AB0858D 022158B3 EF9B5046

StaticUnifiedCDH(B-233)
---
dsU is
000A 0CEEC295
CBE40449 EB555D30 30F852A7 C1F5E1FB C0C8A356 63D67353

QsU_x is
0115 89049EDA
1E0CA97B 74F8F35B C24C7BF0 132F144C EF8118B4 034CD377

QsU_y is
00B9 3DE974B6
BC2D6641 225234C9 EF6FBF4D B755B410 D078B1E2 4B46CB42

dsV is
0044 DD712145
C27DBF0E DAFE8518 B9D5A738 A14CDFE8 D740D3A0 1D8C3AD1

QsV_x is
0063 AA9ECA2E
B58FD095 93B0D822 78604A65 826C23B7 AB0D8E60 5732A0B8

QsV_y is
0153 1A81C7FD
3F10B191 A817B92B FD0AC162 54C07212 F2E9CC55 480889E1

---
no Key Confirmation
NonceU is
00AC F775AE0C
2C707136 0C88D1F3 857D0799 9BD90663 131F3F6E 4190928F

Z is

0112 3BFC0CDD
1E4023CF 8D8B3A98 68ADD850 F2C5E6E0 FB1CF42E 47C5EA6E

OtherInfo is
12345678 9ABCDEF0
414C4943 45313233 E90000AC F775AE0C 2C707136 0C88D1F3
857D0799 9BD90663 131F3F6E 4190928F 424F4242 59343536

DerivedKeyMaterial is
0DB6E2FD 69A150F9
89EB2A2F FC7C66BF EB662A14 0F6882B4 DEF80C53 0A61424F
B31F3408 0C20F44C 4740A274 78AAA99B F5C7396B 2F19D7F5

KeyData is
0DB6E2FD 69A150F9
89EB2A2F FC7C66BF EB662A14 0F6882B4 DEF80C53 0A61424F
B31F3408 0C20F44C 4740A274 78AAA99B F5C7396B 2F19D7F5

Scheme Initiator, Key Confirmation Provider: U to V
NonceU is
00AC F775AE0C
2C707136 0C88D1F3 857D0799 9BD90663 131F3F6E 4190928F

NonceV is
00CE FED290DE
731D6150 04C6659B 940DBD7E DDA88CCE 2B4B180F A0B7BAEF

Z is
0112 3BFC0CDD
1E4023CF 8D8B3A98 68ADD850 F2C5E6E0 FB1CF42E 47C5EA6E

OtherInfo is
12345678 9ABCDEF0
414C4943 45313233 E90000AC F775AE0C 2C707136 0C88D1F3
857D0799 9BD90663 131F3F6E 4190928F 424F4242 59343536

DerivedKeyMaterial is
            0DB6 E2FD69A1 50F989EB 2A2FFC7C 66BFEB66 2A140F68
        82B4DEF8 0C530A61 424FB31F 34080C20 F44C4740 A27478AA
        A99BF5C7 396B2F19 D7F5E245 3DF987CA 462D26C2 1EE9728A

MacData is
                                                        4B435F31
        5F55414C 49434542 4F424259 00ACF775 AE0C2C70 71360C88
        D1F3857D 07999BD9 0663131F 3F6E4190 928F00CE FED290DE
        731D6150 04C6659B 940DBD7E DDA88CCE 2B4B180F A0B7BAEF

MacKey is
                              0DB6 E2FD69A1 50F989EB 2A2FFC7C

Mtag is
                                                        2870A9C5
        009F2728 CB279758 58EAFD87 D4CB2F4D 94B54C32 659E0CE7

KeyData is
                                                66BFEB66 2A140F68
        82B4DEF8 0C530A61 424FB31F 34080C20 F44C4740 A27478AA
        A99BF5C7 396B2F19 D7F5E245 3DF987CA 462D26C2 1EE9728A

Scheme Responder, Key Confirmation Provider: V to U
NonceV is
                                                    00CE FED290DE
        731D6150 04C6659B 940DBD7E DDA88CCE 2B4B180F A0B7BAEF

NonceU is
                                                    00AC F775AE0C
        2C707136 0C88D1F3 857D0799 9BD90663 131F3F6E 4190928F

Z is
                                                    0112 3BFC0CDD
        1E4023CF 8D8B3A98 68ADD850 F2C5E6E0 FB1CF42E 47C5EA6E

```
OtherInfo is
                                                12345678 9ABCDEF0
        414C4943 45313233 E90000AC F775AE0C 2C707136 0C88D1F3
        857D0799 9BD90663 131F3F6E 4190928F 424F4242 59343536


DerivedKeyMaterial is
            0DB6 E2FD69A1 50F989EB 2A2FFC7C 66BFEB66 2A140F68
        82B4DEF8 0C530A61 424FB31F 34080C20 F44C4740 A27478AA
        A99BF5C7 396B2F19 D7F5E245 3DF987CA 462D26C2 1EE9728A


MacData is
            4B43 5F315F56 424F4242 59414C49 434500AC F775AE0C
        2C707136 0C88D1F3 857D0799 9BD90663 131F3F6E 4190928F


MacKey is
                              0DB6 E2FD69A1 50F989EB 2A2FFC7C


Mtag is
                                                        1FB5334E
        7277D415 EF93C8F1 52241537 283653D3 1F8FB88D 2752C66A


KeyData is
                                                66BFEB66 2A140F68
        82B4DEF8 0C530A61 424FB31F 34080C20 F44C4740 A27478AA
        A99BF5C7 396B2F19 D7F5E245 3DF987CA 462D26C2 1EE9728A




------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
NonceU is
                                                    00AC F775AE0C
        2C707136 0C88D1F3 857D0799 9BD90663 131F3F6E 4190928F


NonceV is
                                                    00CE FED290DE
```

```
        731D6150 04C6659B 940DBD7E DDA88CCE 2B4B180F A0B7BAEF


Z is
                                                    0112 3BFC0CDD
        1E4023CF 8D8B3A98 68ADD850 F2C5E6E0 FB1CF42E 47C5EA6E


OtherInfo is
                                                12345678 9ABCDEF0
        414C4943 45313233 E90000AC F775AE0C 2C707136 0C88D1F3
        857D0799 9BD90663 131F3F6E 4190928F 424F4242 59343536


DerivedKeyMaterial is
            0DB6 E2FD69A1 50F989EB 2A2FFC7C 66BFEB66 2A140F68
        82B4DEF8 0C530A61 424FB31F 34080C20 F44C4740 A27478AA
        A99BF5C7 396B2F19 D7F5E245 3DF987CA 462D26C2 1EE9728A


U2V
----------------
MacData is
                                                        4B435F32
        5F55414C 49434542 4F424259 00ACF775 AE0C2C70 71360C88
        D1F3857D 07999BD9 0663131F 3F6E4190 928F00CE FED290DE
        731D6150 04C6659B 940DBD7E DDA88CCE 2B4B180F A0B7BAEF


MacKey is
                                0DB6 E2FD69A1 50F989EB 2A2FFC7C


Mtag is
                                                        7DB46010
        15163614 3D83460D 4D756D99 879FAD43 3B084883 EF1C02AB


V2U
----------------
MacData is
                                                        4B435F32
        5F56424F 42425941 4C494345 00CEFED2 90DE731D 615004C6
        659B940D BD7EDDA8 8CCE2B4B 180FA0B7 BAEF00AC F775AE0C
        2C707136 0C88D1F3 857D0799 9BD90663 131F3F6E 4190928F
```

MacKey is

0DB6 E2FD69A1 50F989EB 2A2FFC7C

Mtag is

23C713D9
AC33C70F 8D5BFC16 4F45F565 6BF4D7C4 83B7B536 1F9A67B2

KeyData is

66BFEB66 2A140F68
82B4DEF8 0C530A61 424FB31F 34080C20 F44C4740 A27478AA
A99BF5C7 396B2F19 D7F5E245 3DF987CA 462D26C2 1EE9728A

FullUnifiedCDH(K-283)
---
dsU is
00DAB643 C868D936 64DC0653
5D912166 CB07985C 5B0D4A9B FDD007AF 7CBBBD2C 43577112

QsU_x is
01101828 5C6ED3BF C8A3DCA4
144C7747 FCFB48CE 1F00B204 36D9A959 8877D601 0A8CE72E

QsU_y is
025F06E6 5C44495D D3C45D69
E951F7BA D5EB52C2 AAF1E3A0 3F64631F 6D810CEA 6BFC0E3E

dsV is
01B4233D EAA8C56E 3872E347
7BB27210 1B190D09 3B596B39 53AC3010 7451F84B 89D0A700

QsV_x is
0543B331 35263633 AD4B9D69
AC7A97A2 CB76DA82 0BFA9842 9E483F6E 117C8C84 0390887D

QsV_y is
066F5A57 B6B52B0D F0B3BC9C
DA64E037 F47EF3EB 71959056 CD2E7121 3FD8EDEE 549E2098

deU is
00F7C6B3 BE198B33 AC66FDAA
529278F6 D9CF9226 954DCF7B 4B334AF6 2E37C242 91F0E5A3

QeU_x is
06826AD1 C80EC52B A5ED422E
BCEB4E1A C9BF4815 9213BCF0 1EECB4CA 8ECC2147 8F2E4E62

QeU_y is
0205EA96 61435B98 AF972801

```
        24824B4E AE66D297 A45D89C5 541576B0 25AF34EF 021AF04B


deV is
                                  013EFD36 5B268B47 C218FA3A
        DFBD7A89 68B561D7 2169EFF3 8A24B9E9 B1975E07 90168A79


QeV_x is
                                  03741722 B1DB15B8 2058DF77
        FE4A98AD 46FA9D81 B8663740 5CDF7630 42ADEDE3 EA519C88


QeV_y is
                                  06221454 F3715018 5994B87E
        6774908F 9EDF6326 A68983A6 A2E8E907 4868E5CF 19BD1C2D




------------------------------------------------------------
no Key Confirmation
Zs is
                                  0260FB0F DC1F6140 DF548306
        8D276BB4 F704C092 89D5624C F432EDB2 6D4EE78C 77209FB7


Ze is
                                  04C0A765 3CD0B588 9E578D13
        6B5561C1 7A004D53 4126BB3E 7668B322 30BCB2F4 47E1C96B


Z is
        04C0A765 3CD0B588 9E578D13 6B5561C1 7A004D53 4126BB3E
        7668B322 30BCB2F4 47E1C96B 0260FB0F DC1F6140 DF548306
        8D276BB4 F704C092 89D5624C F432EDB2 6D4EE78C 77209FB7


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                          5E14B569 4B65001E D940BDB1 3607CFC4
        AEF35290 CC86F116 24C6F84D C2FDDECB 7813CFEB 882D5562
        A6051ABD 050502FB B30A9627 55A39F95 7409A566 1246703E
```

KeyData is
                          5E14B569 4B65001E D940BDB1 3607CFC4
        AEF35290 CC86F116 24C6F84D C2FDDECB 7813CFEB 882D5562
        A6051ABD 050502FB B30A9627 55A39F95 7409A566 1246703E

Scheme Initiator, Key Confirmation Provider: U to V
Zs is
                                  0260FB0F DC1F6140 DF548306
        8D276BB4 F704C092 89D5624C F432EDB2 6D4EE78C 77209FB7

Ze is
                                  04C0A765 3CD0B588 9E578D13
        6B5561C1 7A004D53 4126BB3E 7668B322 30BCB2F4 47E1C96B

Z is
        04C0A765 3CD0B588 9E578D13 6B5561C1 7A004D53 4126BB3E
        7668B322 30BCB2F4 47E1C96B 0260FB0F DC1F6140 DF548306
        8D276BB4 F704C092 89D5624C F432EDB2 6D4EE78C 77209FB7

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                                                5E14B569 4B65001E
        D940BDB1 3607CFC4 AEF35290 CC86F116 24C6F84D C2FDDECB
        7813CFEB 882D5562 A6051ABD 050502FB B30A9627 55A39F95
        7409A566 1246703E 9C4F6729 73AA9B70 25A2C706 E4D3974D

MacData is
                          4B435F31 5F55414C 49434542 4F424259
        06826AD1 C80EC52B A5ED422E BCEB4E1A C9BF4815 9213BCF0
        1EECB4CA 8ECC2147 8F2E4E62 0205EA96 61435B98 AF972801
        24824B4E AE66D297 A45D89C5 541576B0 25AF34EF 021AF04B
        03741722 B1DB15B8 2058DF77 FE4A98AD 46FA9D81 B8663740
        5CDF7630 42ADEDE3 EA519C88 06221454 F3715018 5994B87E

6774908F 9EDF6326 A68983A6 A2E8E907 4868E5CF 19BD1C2D

MacKey is
5E14B569 4B65001E D940BDB1 3607CFC4

Mtag is
95B83EDA F961EC90
7635AD02 C06171C5 9422AEBD 434F5CA1 67B39673 4CBA2769

KeyData is
AEF35290 CC86F116 24C6F84D C2FDDECB
7813CFEB 882D5562 A6051ABD 050502FB B30A9627 55A39F95
7409A566 1246703E 9C4F6729 73AA9B70 25A2C706 E4D3974D

Scheme Responder, Key Confirmation Provider: V to U
Zs is
0260FB0F DC1F6140 DF548306
8D276BB4 F704C092 89D5624C F432EDB2 6D4EE78C 77209FB7

Ze is
04C0A765 3CD0B588 9E578D13
6B5561C1 7A004D53 4126BB3E 7668B322 30BCB2F4 47E1C96B

Z is
04C0A765 3CD0B588 9E578D13 6B5561C1 7A004D53 4126BB3E
7668B322 30BCB2F4 47E1C96B 0260FB0F DC1F6140 DF548306
8D276BB4 F704C092 89D5624C F432EDB2 6D4EE78C 77209FB7

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
5E14B569 4B65001E
D940BDB1 3607CFC4 AEF35290 CC86F116 24C6F84D C2FDDECB
7813CFEB 882D5562 A6051ABD 050502FB B30A9627 55A39F95

```
        7409A566 1246703E 9C4F6729 73AA9B70 25A2C706 E4D3974D


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        03741722 B1DB15B8 2058DF77 FE4A98AD 46FA9D81 B8663740
        5CDF7630 42ADEDE3 EA519C88 06221454 F3715018 5994B87E
        6774908F 9EDF6326 A68983A6 A2E8E907 4868E5CF 19BD1C2D
        06826AD1 C80EC52B A5ED422E BCEB4E1A C9BF4815 9213BCF0
        1EECB4CA 8ECC2147 8F2E4E62 0205EA96 61435B98 AF972801
        24824B4E AE66D297 A45D89C5 541576B0 25AF34EF 021AF04B


MacKey is
                         5E14B569 4B65001E D940BDB1 3607CFC4


Mtag is
                                             A01125AF 092BDD43
        189DB65F 40BCD4A9 5693EEF0 C785C4D9 1F991EB9 91CBD4C1


KeyData is
                         AEF35290 CC86F116 24C6F84D C2FDDECB
        7813CFEB 882D5562 A6051ABD 050502FB B30A9627 55A39F95
        7409A566 1246703E 9C4F6729 73AA9B70 25A2C706 E4D3974D




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
Zs is
                                   0260FB0F DC1F6140 DF548306
        8D276BB4 F704C092 89D5624C F432EDB2 6D4EE78C 77209FB7


Ze is
                                   04C0A765 3CD0B588 9E578D13
        6B5561C1 7A004D53 4126BB3E 7668B322 30BCB2F4 47E1C96B


Z is
        04C0A765 3CD0B588 9E578D13 6B5561C1 7A004D53 4126BB3E
        7668B322 30BCB2F4 47E1C96B 0260FB0F DC1F6140 DF548306
        8D276BB4 F704C092 89D5624C F432EDB2 6D4EE78C 77209FB7
```

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                 5E14B569 4B65001E
        D940BDB1 3607CFC4 AEF35290 CC86F116 24C6F84D C2FDDECB
        7813CFEB 882D5562 A6051ABD 050502FB B30A9627 55A39F95
        7409A566 1246703E 9C4F6729 73AA9B70 25A2C706 E4D3974D


U2V
----------------
MacData is
                         4B435F32 5F55414C 49434542 4F424259
        06826AD1 C80EC52B A5ED422E BCEB4E1A C9BF4815 9213BCF0
        1EECB4CA 8ECC2147 8F2E4E62 0205EA96 61435B98 AF972801
        24824B4E AE66D297 A45D89C5 541576B0 25AF34EF 021AF04B
        03741722 B1DB15B8 2058DF77 FE4A98AD 46FA9D81 B8663740
        5CDF7630 42ADEDE3 EA519C88 06221454 F3715018 5994B87E
        6774908F 9EDF6326 A68983A6 A2E8E907 4868E5CF 19BD1C2D


MacKey is
                         5E14B569 4B65001E D940BDB1 3607CFC4


Mtag is
                                                 71187FBA 08E9DBF5
        B3CD9BBE EC729BEC 50957588 8F301EE6 9516E229 FFD5273C


V2U
----------------
MacData is
                         4B435F32 5F56424F 42425941 4C494345
        03741722 B1DB15B8 2058DF77 FE4A98AD 46FA9D81 B8663740
        5CDF7630 42ADEDE3 EA519C88 06221454 F3715018 5994B87E
        6774908F 9EDF6326 A68983A6 A2E8E907 4868E5CF 19BD1C2D
        06826AD1 C80EC52B A5ED422E BCEB4E1A C9BF4815 9213BCF0
        1EECB4CA 8ECC2147 8F2E4E62 0205EA96 61435B98 AF972801
        24824B4E AE66D297 A45D89C5 541576B0 25AF34EF 021AF04B
```

```
MacKey is
                         5E14B569 4B65001E D940BDB1 3607CFC4


Mtag is
                                                  B6681831 FAA50037
        96766CD0 3B202C6D 7745D931 96563719 CE193E04 629C9D3B


KeyData is
                         AEF35290 CC86F116 24C6F84D C2FDDECB
        7813CFEB 882D5562 A6051ABD 050502FB B30A9627 55A39F95
        7409A566 1246703E 9C4F6729 73AA9B70 25A2C706 E4D3974D




FullMQV(K-283)
-------------------------------------------------------------
dsU is
                                  00DAB643 C868D936 64DC0653
        5D912166 CB07985C 5B0D4A9B FDD007AF 7CBBBD2C 43577112


QsU_x is
                                  01101828 5C6ED3BF C8A3DCA4
        144C7747 FCFB48CE 1F00B204 36D9A959 8877D601 0A8CE72E


QsU_y is
                                  025F06E6 5C44495D D3C45D69
        E951F7BA D5EB52C2 AAF1E3A0 3F64631F 6D810CEA 6BFC0E3E


dsV is
                                  01B4233D EAA8C56E 3872E347
        7BB27210 1B190D09 3B596B39 53AC3010 7451F84B 89D0A700


QsV_x is
                                  0543B331 35263633 AD4B9D69
        AC7A97A2 CB76DA82 0BFA9842 9E483F6E 117C8C84 0390887D


QsV_y is
                                  066F5A57 B6B52B0D F0B3BC9C
```

DA64E037 F47EF3EB 71959056 CD2E7121 3FD8EDEE 549E2098

deU is
00F7C6B3 BE198B33 AC66FDAA
529278F6 D9CF9226 954DCF7B 4B334AF6 2E37C242 91F0E5A3

QeU_x is
06826AD1 C80EC52B A5ED422E
BCEB4E1A C9BF4815 9213BCF0 1EECB4CA 8ECC2147 8F2E4E62

QeU_y is
0205EA96 61435B98 AF972801
24824B4E AE66D297 A45D89C5 541576B0 25AF34EF 021AF04B

deV is
013EFD36 5B268B47 C218FA3A
DFBD7A89 68B561D7 2169EFF3 8A24B9E9 B1975E07 90168A79

QeV_x is
03741722 B1DB15B8 2058DF77
FE4A98AD 46FA9D81 B8663740 5CDF7630 42ADEDE3 EA519C88

QeV_y is
06221454 F3715018 5994B87E
6774908F 9EDF6326 A68983A6 A2E8E907 4868E5CF 19BD1C2D

---

no Key Confirmation
Z is
01DA061D 0B5C3512 09DF3919
58A8825F 3BBAE2CD 5AC4C1B5 B74CE702 A4C38FFF C53C00EA

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

```
DerivedKeyMaterial is
                          8810F806 2B0DFE5F D0B357E1 33D2A2CB
        75DE71CD E853F7C1 46C6A612 9E269A69 56DDF4F3 3000FB26
        FC58BA92 A7FA5937 FA41CFDC C61C23AE E74B5DC4 804D2086


KeyData is
                          8810F806 2B0DFE5F D0B357E1 33D2A2CB
        75DE71CD E853F7C1 46C6A612 9E269A69 56DDF4F3 3000FB26
        FC58BA92 A7FA5937 FA41CFDC C61C23AE E74B5DC4 804D2086




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Z is
                                  01DA061D 0B5C3512 09DF3919
        58A8825F 3BBAE2CD 5AC4C1B5 B74CE702 A4C38FFF C53C00EA


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                 8810F806 2B0DFE5F
        D0B357E1 33D2A2CB 75DE71CD E853F7C1 46C6A612 9E269A69
        56DDF4F3 3000FB26 FC58BA92 A7FA5937 FA41CFDC C61C23AE
        E74B5DC4 804D2086 C162A289 5A1902EB 3569D134 A71546E1


MacData is
                          4B435F31 5F55414C 49434542 4F424259
        06826AD1 C80EC52B A5ED422E BCEB4E1A C9BF4815 9213BCF0
        1EECB4CA 8ECC2147 8F2E4E62 0205EA96 61435B98 AF972801
        24824B4E AE66D297 A45D89C5 541576B0 25AF34EF 021AF04B
        03741722 B1DB15B8 2058DF77 FE4A98AD 46FA9D81 B8663740
        5CDF7630 42ADEDE3 EA519C88 06221454 F3715018 5994B87E
        6774908F 9EDF6326 A68983A6 A2E8E907 4868E5CF 19BD1C2D


MacKey is
                          8810F806 2B0DFE5F D0B357E1 33D2A2CB
```

Mtag is
                                                92FDD17A 55D2798E
        BB3E7CF6 D642EFD5 EA7112DE 87422276 63EF7263 96A5BD58

KeyData is
                            75DE71CD E853F7C1 46C6A612 9E269A69
        56DDF4F3 3000FB26 FC58BA92 A7FA5937 FA41CFDC C61C23AE
        E74B5DC4 804D2086 C162A289 5A1902EB 3569D134 A71546E1

Scheme Responder, Key Confirmation Provider: V to U
Z is
                                    01DA061D 0B5C3512 09DF3919
        58A8825F 3BBAE2CD 5AC4C1B5 B74CE702 A4C38FFF C53C00EA

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                                                8810F806 2B0DFE5F
        D0B357E1 33D2A2CB 75DE71CD E853F7C1 46C6A612 9E269A69
        56DDF4F3 3000FB26 FC58BA92 A7FA5937 FA41CFDC C61C23AE
        E74B5DC4 804D2086 C162A289 5A1902EB 3569D134 A71546E1

MacData is
                            4B435F31 5F56424F 42425941 4C494345
        03741722 B1DB15B8 2058DF77 FE4A98AD 46FA9D81 B8663740
        5CDF7630 42ADEDE3 EA519C88 06221454 F3715018 5994B87E
        6774908F 9EDF6326 A68983A6 A2E8E907 4868E5CF 19BD1C2D
        06826AD1 C80EC52B A5ED422E BCEB4E1A C9BF4815 9213BCF0
        1EECB4CA 8ECC2147 8F2E4E62 0205EA96 61435B98 AF972801
        24824B4E AE66D297 A45D89C5 541576B0 25AF34EF 021AF04B

MacKey is
                            8810F806 2B0DFE5F D0B357E1 33D2A2CB

Mtag is

```
                                                2DF37C5E 7C2F58B0
        62ED816A 1188FFB1 29E262AC F13A2CB8 1860687D C667EF94


KeyData is
                           75DE71CD E853F7C1 46C6A612 9E269A69
        56DDF4F3 3000FB26 FC58BA92 A7FA5937 FA41CFDC C61C23AE
        E74B5DC4 804D2086 C162A289 5A1902EB 3569D134 A71546E1




------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
Z is
                                    01DA061D 0B5C3512 09DF3919
        58A8825F 3BBAE2CD 5AC4C1B5 B74CE702 A4C38FFF C53C00EA


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                8810F806 2B0DFE5F
        D0B357E1 33D2A2CB 75DE71CD E853F7C1 46C6A612 9E269A69
        56DDF4F3 3000FB26 FC58BA92 A7FA5937 FA41CFDC C61C23AE
        E74B5DC4 804D2086 C162A289 5A1902EB 3569D134 A71546E1


U2V
----------------
MacData is
                           4B435F32 5F55414C 49434542 4F424259
        06826AD1 C80EC52B A5ED422E BCEB4E1A C9BF4815 9213BCF0
        1EECB4CA 8ECC2147 8F2E4E62 0205EA96 61435B98 AF972801
        24824B4E AE66D297 A45D89C5 541576B0 25AF34EF 021AF04B
        03741722 B1DB15B8 2058DF77 FE4A98AD 46FA9D81 B8663740
        5CDF7630 42ADEDE3 EA519C88 06221454 F3715018 5994B87E
        6774908F 9EDF6326 A68983A6 A2E8E907 4868E5CF 19BD1C2D


MacKey is
                           8810F806 2B0DFE5F D0B357E1 33D2A2CB
```

```
Mtag is
                                                F66CA5D3 2732DF7B
        7AD46DC2 61369F2E 6C0E7C5C FDA313B0 AE702E47 11878FBF


V2U
----------------
MacData is
                         4B435F32 5F56424F 42425941 4C494345
        03741722 B1DB15B8 2058DF77 FE4A98AD 46FA9D81 B8663740
        5CDF7630 42ADEDE3 EA519C88 06221454 F3715018 5994B87E
        6774908F 9EDF6326 A68983A6 A2E8E907 4868E5CF 19BD1C2D
        06826AD1 C80EC52B A5ED422E BCEB4E1A C9BF4815 9213BCF0
        1EECB4CA 8ECC2147 8F2E4E62 0205EA96 61435B98 AF972801
        24824B4E AE66D297 A45D89C5 541576B0 25AF34EF 021AF04B


MacKey is
                         8810F806 2B0DFE5F D0B357E1 33D2A2CB


Mtag is
                                                5F584D83 CA8D5C41
        9143251E FAC82FF3 8874B293 B9762D46 3A6DC25B 1677E6AC


KeyData is
                         75DE71CD E853F7C1 46C6A612 9E269A69
        56DDF4F3 3000FB26 FC58BA92 A7FA5937 FA41CFDC C61C23AE
        E74B5DC4 804D2086 C162A289 5A1902EB 3569D134 A71546E1




EphemeralUnifiedCDH(K-283)
------------------------------------------------------------
deU is
                                    00F7C6B3 BE198B33 AC66FDAA
        529278F6 D9CF9226 954DCF7B 4B334AF6 2E37C242 91F0E5A3


QeU_x is
                                    06826AD1 C80EC52B A5ED422E
        BCEB4E1A C9BF4815 9213BCF0 1EECB4CA 8ECC2147 8F2E4E62
```

```
QeU_y is
                                0205EA96 61435B98 AF972801
        24824B4E AE66D297 A45D89C5 541576B0 25AF34EF 021AF04B


deV is
                                013EFD36 5B268B47 C218FA3A
        DFBD7A89 68B561D7 2169EFF3 8A24B9E9 B1975E07 90168A79


QeV_x is
                                03741722 B1DB15B8 2058DF77
        FE4A98AD 46FA9D81 B8663740 5CDF7630 42ADEDE3 EA519C88


QeV_y is
                                06221454 F3715018 5994B87E
        6774908F 9EDF6326 A68983A6 A2E8E907 4868E5CF 19BD1C2D




------------------------------------------------------------
no Key Confirmation
Z is
                                04C0A765 3CD0B588 9E578D13
        6B5561C1 7A004D53 4126BB3E 7668B322 30BCB2F4 47E1C96B


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                            D8E92475 CAC39F4D B0518821 53C683E6
        3B13D8CF 0F9B3E97 66ADA6F5 94359B0D 9D2BA45F 24852366
        EF291404 C81C502C 491C55F5 31A497E0 F55CD4F1 A66E64D6


KeyData is
                            D8E92475 CAC39F4D B0518821 53C683E6
        3B13D8CF 0F9B3E97 66ADA6F5 94359B0D 9D2BA45F 24852366
        EF291404 C81C502C 491C55F5 31A497E0 F55CD4F1 A66E64D6
```

OnePassUnifiedCDH(K-283)
---
dsU is
00DAB643 C868D936 64DC0653
5D912166 CB07985C 5B0D4A9B FDD007AF 7CBBBD2C 43577112

QsU_x is
01101828 5C6ED3BF C8A3DCA4
144C7747 FCFB48CE 1F00B204 36D9A959 8877D601 0A8CE72E

QsU_y is
025F06E6 5C44495D D3C45D69
E951F7BA D5EB52C2 AAF1E3A0 3F64631F 6D810CEA 6BFC0E3E

dsV is
01B4233D EAA8C56E 3872E347
7BB27210 1B190D09 3B596B39 53AC3010 7451F84B 89D0A700

QsV_x is
0543B331 35263633 AD4B9D69
AC7A97A2 CB76DA82 0BFA9842 9E483F6E 117C8C84 0390887D

QsV_y is
066F5A57 B6B52B0D F0B3BC9C
DA64E037 F47EF3EB 71959056 CD2E7121 3FD8EDEE 549E2098

deU is
00F7C6B3 BE198B33 AC66FDAA
529278F6 D9CF9226 954DCF7B 4B334AF6 2E37C242 91F0E5A3

QeU_x is
06826AD1 C80EC52B A5ED422E
BCEB4E1A C9BF4815 9213BCF0 1EECB4CA 8ECC2147 8F2E4E62

QeU_y is
0205EA96 61435B98 AF972801

```
        24824B4E AE66D297 A45D89C5 541576B0 25AF34EF 021AF04B



------------------------------------------------------------
no Key Confirmation
Zs is
                                  0260FB0F DC1F6140 DF548306
        8D276BB4 F704C092 89D5624C F432EDB2 6D4EE78C 77209FB7


Ze is
                                  0091A6BD 5E5C5EF6 48C34B14
        72E6F2F9 C80D1D85 EE2DE0BD E5361921 AA34D915 87A145EF


Z is
        0091A6BD 5E5C5EF6 48C34B14 72E6F2F9 C80D1D85 EE2DE0BD
        E5361921 AA34D915 87A145EF 0260FB0F DC1F6140 DF548306
        8D276BB4 F704C092 89D5624C F432EDB2 6D4EE78C 77209FB7


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                          98F02843 906155A8 FB5226FB 4D4A7EFB
        DBA56783 BA7E4E2D 022880CD CB666678 D0F30FA2 F389B32E
        D527B8F2 326EFF76 CC3BAD88 EF38ACB9 7090AB43 D3DA0526


KeyData is
                          98F02843 906155A8 FB5226FB 4D4A7EFB
        DBA56783 BA7E4E2D 022880CD CB666678 D0F30FA2 F389B32E
        D527B8F2 326EFF76 CC3BAD88 EF38ACB9 7090AB43 D3DA0526



------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                                  01570933 A3C886AA 674F4D0B
        65B0CADE 72A3CE5C 4074DC8F 3ECCDC2E 684766D3 968328D3
```

```
Zs is
                                0260FB0F DC1F6140 DF548306
        8D276BB4 F704C092 89D5624C F432EDB2 6D4EE78C 77209FB7


Ze is
                                0091A6BD 5E5C5EF6 48C34B14
        72E6F2F9 C80D1D85 EE2DE0BD E5361921 AA34D915 87A145EF


Z is
        0091A6BD 5E5C5EF6 48C34B14 72E6F2F9 C80D1D85 EE2DE0BD
        E5361921 AA34D915 87A145EF 0260FB0F DC1F6140 DF548306
        8D276BB4 F704C092 89D5624C F432EDB2 6D4EE78C 77209FB7


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                            98F02843 906155A8
        FB5226FB 4D4A7EFB DBA56783 BA7E4E2D 022880CD CB666678
        D0F30FA2 F389B32E D527B8F2 326EFF76 CC3BAD88 EF38ACB9
        7090AB43 D3DA0526 1A44AD90 C25E0EC9 C69AD790 2A8E324D


MacData is
                                                    4B435F31
        5F55414C 49434542 4F424259 06826AD1 C80EC52B A5ED422E
        BCEB4E1A C9BF4815 9213BCF0 1EECB4CA 8ECC2147 8F2E4E62
        0205EA96 61435B98 AF972801 24824B4E AE66D297 A45D89C5
        541576B0 25AF34EF 021AF04B 01570933 A3C886AA 674F4D0B
        65B0CADE 72A3CE5C 4074DC8F 3ECCDC2E 684766D3 968328D3


MacKey is
                        98F02843 906155A8 FB5226FB 4D4A7EFB


Mtag is
                                            359A03E0 4E5C699A
        80C44B82 23BE9201 1C5860A2 BF450810 5366992E E2D461E0
```

KeyData is
                        DBA56783 BA7E4E2D 022880CD CB666678
        D0F30FA2 F389B32E D527B8F2 326EFF76 CC3BAD88 EF38ACB9
        7090AB43 D3DA0526 1A44AD90 C25E0EC9 C69AD790 2A8E324D

Scheme Responder, Key Confirmation Provider: V to U
NonceU is
                                    01570933 A3C886AA 674F4D0B
        65B0CADE 72A3CE5C 4074DC8F 3ECCDC2E 684766D3 968328D3

Zs is
                                    0260FB0F DC1F6140 DF548306
        8D276BB4 F704C092 89D5624C F432EDB2 6D4EE78C 77209FB7

Ze is
                                    0091A6BD 5E5C5EF6 48C34B14
        72E6F2F9 C80D1D85 EE2DE0BD E5361921 AA34D915 87A145EF

Z is
        0091A6BD 5E5C5EF6 48C34B14 72E6F2F9 C80D1D85 EE2DE0BD
        E5361921 AA34D915 87A145EF 0260FB0F DC1F6140 DF548306
        8D276BB4 F704C092 89D5624C F432EDB2 6D4EE78C 77209FB7

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                                                98F02843 906155A8
        FB5226FB 4D4A7EFB DBA56783 BA7E4E2D 022880CD CB666678
        D0F30FA2 F389B32E D527B8F2 326EFF76 CC3BAD88 EF38ACB9
        7090AB43 D3DA0526 1A44AD90 C25E0EC9 C69AD790 2A8E324D

MacData is
                        4B435F31 5F56424F 42425941 4C494345
        06826AD1 C80EC52B A5ED422E BCEB4E1A C9BF4815 9213BCF0

```
        1EECB4CA 8ECC2147 8F2E4E62 0205EA96 61435B98 AF972801
        24824B4E AE66D297 A45D89C5 541576B0 25AF34EF 021AF04B


MacKey is
                         98F02843 906155A8 FB5226FB 4D4A7EFB


Mtag is
                                            C9FFB2C6 BA949DE9
        63393E4E EAF7636C 86C075AA 3D4AFF6F 8F8E344E A8EBF743


KeyData is
                         DBA56783 BA7E4E2D 022880CD CB666678
        D0F30FA2 F389B32E D527B8F2 326EFF76 CC3BAD88 EF38ACB9
        7090AB43 D3DA0526 1A44AD90 C25E0EC9 C69AD790 2A8E324D




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
                                    01570933 A3C886AA 674F4D0B
        65B0CADE 72A3CE5C 4074DC8F 3ECCDC2E 684766D3 968328D3


Zs is
                                    0260FB0F DC1F6140 DF548306
        8D276BB4 F704C092 89D5624C F432EDB2 6D4EE78C 77209FB7


Ze is
                                    0091A6BD 5E5C5EF6 48C34B14
        72E6F2F9 C80D1D85 EE2DE0BD E5361921 AA34D915 87A145EF


Z is
        0091A6BD 5E5C5EF6 48C34B14 72E6F2F9 C80D1D85 EE2DE0BD
        E5361921 AA34D915 87A145EF 0260FB0F DC1F6140 DF548306
        8D276BB4 F704C092 89D5624C F432EDB2 6D4EE78C 77209FB7


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536
```

```
DerivedKeyMaterial is
                                                98F02843 906155A8
        FB5226FB 4D4A7EFB DBA56783 BA7E4E2D 022880CD CB666678
        D0F30FA2 F389B32E D527B8F2 326EFF76 CC3BAD88 EF38ACB9
        7090AB43 D3DA0526 1A44AD90 C25E0EC9 C69AD790 2A8E324D


U2V
----------------
MacData is
                                                        4B435F32
        5F55414C 49434542 4F424259 06826AD1 C80EC52B A5ED422E
        BCEB4E1A C9BF4815 9213BCF0 1EECB4CA 8ECC2147 8F2E4E62
        0205EA96 61435B98 AF972801 24824B4E AE66D297 A45D89C5
        541576B0 25AF34EF 021AF04B 01570933 A3C886AA 674F4D0B
        65B0CADE 72A3CE5C 4074DC8F 3ECCDC2E 684766D3 968328D3


MacKey is
                        98F02843 906155A8 FB5226FB 4D4A7EFB


Mtag is
                                                FB6494E5 31AD8D26
        F372A02B 899CFA70 64A8D062 6F88C581 B3AD2DBC CB0B3085


V2U
----------------
MacData is
                                                        4B435F32
        5F56424F 42425941 4C494345 01570933 A3C886AA 674F4D0B
        65B0CADE 72A3CE5C 4074DC8F 3ECCDC2E 684766D3 968328D3
        06826AD1 C80EC52B A5ED422E BCEB4E1A C9BF4815 9213BCF0
        1EECB4CA 8ECC2147 8F2E4E62 0205EA96 61435B98 AF972801
        24824B4E AE66D297 A45D89C5 541576B0 25AF34EF 021AF04B


MacKey is
                        98F02843 906155A8 FB5226FB 4D4A7EFB


Mtag is
                                                B4EB3C4D 14364343
```

```
        3D863FFE A6CE5FDB CE3CCF7E F3BCBB24 AE6A0E5F EB362E30


KeyData is
                          DBA56783 BA7E4E2D 022880CD CB666678
        D0F30FA2 F389B32E D527B8F2 326EFF76 CC3BAD88 EF38ACB9
        7090AB43 D3DA0526 1A44AD90 C25E0EC9 C69AD790 2A8E324D




OnePassMQV(K-283)
------------------------------------------------------------
dsU is
                                   00DAB643 C868D936 64DC0653
        5D912166 CB07985C 5B0D4A9B FDD007AF 7CBBBD2C 43577112


QsU_x is
                                   01101828 5C6ED3BF C8A3DCA4
        144C7747 FCFB48CE 1F00B204 36D9A959 8877D601 0A8CE72E


QsU_y is
                                   025F06E6 5C44495D D3C45D69
        E951F7BA D5EB52C2 AAF1E3A0 3F64631F 6D810CEA 6BFC0E3E


dsV is
                                   01B4233D EAA8C56E 3872E347
        7BB27210 1B190D09 3B596B39 53AC3010 7451F84B 89D0A700


QsV_x is
                                   0543B331 35263633 AD4B9D69
        AC7A97A2 CB76DA82 0BFA9842 9E483F6E 117C8C84 0390887D


QsV_y is
                                   066F5A57 B6B52B0D F0B3BC9C
        DA64E037 F47EF3EB 71959056 CD2E7121 3FD8EDEE 549E2098


deU is
                                   00F7C6B3 BE198B33 AC66FDAA
        529278F6 D9CF9226 954DCF7B 4B334AF6 2E37C242 91F0E5A3
```

```
QeU_x is
                                    06826AD1 C80EC52B A5ED422E
        BCEB4E1A C9BF4815 9213BCF0 1EECB4CA 8ECC2147 8F2E4E62


QeU_y is
                                    0205EA96 61435B98 AF972801
        24824B4E AE66D297 A45D89C5 541576B0 25AF34EF 021AF04B




------------------------------------------------------------
no Key Confirmation
Z is
                                    076DE3B9 65AAA91D 4FE0CC3D
        DF7AEBAD 6139B1C0 0A50867E 8AC09CA1 5FCF467A 3556E783


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                            82A1F068 C8A1E39F 9D7D76A1 DDD0CD0F
        05038891 D0D5E6B0 FBB4A12C 8A43229B 9EAE43DA 6311F239
        D8271D9A 96C89B00 7C55B754 DF510A3C 4ED8B084 26EBD954


KeyData is
                            82A1F068 C8A1E39F 9D7D76A1 DDD0CD0F
        05038891 D0D5E6B0 FBB4A12C 8A43229B 9EAE43DA 6311F239
        D8271D9A 96C89B00 7C55B754 DF510A3C 4ED8B084 26EBD954




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                                    01570933 A3C886AA 674F4D0B
        65B0CADE 72A3CE5C 4074DC8F 3ECCDC2E 684766D3 968328D3
```

```
Z is
                                    076DE3B9 65AAA91D 4FE0CC3D
        DF7AEBAD 6139B1C0 0A50867E 8AC09CA1 5FCF467A 3556E783


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                              82A1F068 C8A1E39F
        9D7D76A1 DDD0CD0F 05038891 D0D5E6B0 FBB4A12C 8A43229B
        9EAE43DA 6311F239 D8271D9A 96C89B00 7C55B754 DF510A3C
        4ED8B084 26EBD954 1C2ACB5D 80575DD8 B7D45EF0 C7368783


MacData is
                                                        4B435F31
        5F55414C 49434542 4F424259 06826AD1 C80EC52B A5ED422E
        BCEB4E1A C9BF4815 9213BCF0 1EECB4CA 8ECC2147 8F2E4E62
        0205EA96 61435B98 AF972801 24824B4E AE66D297 A45D89C5
        541576B0 25AF34EF 021AF04B 01570933 A3C886AA 674F4D0B
        65B0CADE 72A3CE5C 4074DC8F 3ECCDC2E 684766D3 968328D3


MacKey is
                           82A1F068 C8A1E39F 9D7D76A1 DDD0CD0F


Mtag is
                                              3DF75BB0 67EF53C0
        BB48BD97 35B068E9 EE54DB7C 11A02877 3861EFA7 9F9030F2


KeyData is
                           05038891 D0D5E6B0 FBB4A12C 8A43229B
        9EAE43DA 6311F239 D8271D9A 96C89B00 7C55B754 DF510A3C
        4ED8B084 26EBD954 1C2ACB5D 80575DD8 B7D45EF0 C7368783




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
                                    01570933 A3C886AA 674F4D0B
```

```
        65B0CADE 72A3CE5C 4074DC8F 3ECCDC2E 684766D3 968328D3


Z is
                                  076DE3B9 65AAA91D 4FE0CC3D
        DF7AEBAD 6139B1C0 0A50867E 8AC09CA1 5FCF467A 3556E783


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                            82A1F068 C8A1E39F
        9D7D76A1 DDD0CD0F 05038891 D0D5E6B0 FBB4A12C 8A43229B
        9EAE43DA 6311F239 D8271D9A 96C89B00 7C55B754 DF510A3C
        4ED8B084 26EBD954 1C2ACB5D 80575DD8 B7D45EF0 C7368783


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        06826AD1 C80EC52B A5ED422E BCEB4E1A C9BF4815 9213BCF0
        1EECB4CA 8ECC2147 8F2E4E62 0205EA96 61435B98 AF972801
        24824B4E AE66D297 A45D89C5 541576B0 25AF34EF 021AF04B


MacKey is
                         82A1F068 C8A1E39F 9D7D76A1 DDD0CD0F


Mtag is
                                            C02F2F57 B22DA54E
        3AB5B589 7ED67A7F E4B68E70 7497AC0F 10DDFF8D 121E7CDC


KeyData is
                         05038891 D0D5E6B0 FBB4A12C 8A43229B
        9EAE43DA 6311F239 D8271D9A 96C89B00 7C55B754 DF510A3C
        4ED8B084 26EBD954 1C2ACB5D 80575DD8 B7D45EF0 C7368783




-------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
```

```
                                    01570933 A3C886AA 674F4D0B
        65B0CADE 72A3CE5C 4074DC8F 3ECCDC2E 684766D3 968328D3


Z is
                                    076DE3B9 65AAA91D 4FE0CC3D
        DF7AEBAD 6139B1C0 0A50867E 8AC09CA1 5FCF467A 3556E783


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                82A1F068 C8A1E39F
        9D7D76A1 DDD0CD0F 05038891 D0D5E6B0 FBB4A12C 8A43229B
        9EAE43DA 6311F239 D8271D9A 96C89B00 7C55B754 DF510A3C
        4ED8B084 26EBD954 1C2ACB5D 80575DD8 B7D45EF0 C7368783


U2V
----------------
MacData is
                                                        4B435F32
        5F55414C 49434542 4F424259 06826AD1 C80EC52B A5ED422E
        BCEB4E1A C9BF4815 9213BCF0 1EECB4CA 8ECC2147 8F2E4E62
        0205EA96 61435B98 AF972801 24824B4E AE66D297 A45D89C5
        541576B0 25AF34EF 021AF04B 01570933 A3C886AA 674F4D0B
        65B0CADE 72A3CE5C 4074DC8F 3ECCDC2E 684766D3 968328D3


MacKey is
                           82A1F068 C8A1E39F 9D7D76A1 DDD0CD0F


Mtag is
                                                F843C01B BF1CFDDD
        766C24F3 9FDC80D8 BD3F0BD0 97D74F05 7F988F5E F0C3C892


V2U
----------------
MacData is
                                                        4B435F32
        5F56424F 42425941 4C494345 01570933 A3C886AA 674F4D0B
        65B0CADE 72A3CE5C 4074DC8F 3ECCDC2E 684766D3 968328D3
```

06826AD1 C80EC52B A5ED422E BCEB4E1A C9BF4815 9213BCF0
1EECB4CA 8ECC2147 8F2E4E62 0205EA96 61435B98 AF972801
24824B4E AE66D297 A45D89C5 541576B0 25AF34EF 021AF04B

MacKey is
82A1F068 C8A1E39F 9D7D76A1 DDD0CD0F

Mtag is
DEFDF24C C69542AA
12606AA1 E7729F8B E6CDB1AF 4966400C C8B18229 257ED4C9

KeyData is
05038891 D0D5E6B0 FBB4A12C 8A43229B
9EAE43DA 6311F239 D8271D9A 96C89B00 7C55B754 DF510A3C
4ED8B084 26EBD954 1C2ACB5D 80575DD8 B7D45EF0 C7368783

OnePassDiffieHellmanCDH(K-283)
---
dsV is
01B4233D EAA8C56E 3872E347
7BB27210 1B190D09 3B596B39 53AC3010 7451F84B 89D0A700

QsV_x is
0543B331 35263633 AD4B9D69
AC7A97A2 CB76DA82 0BFA9842 9E483F6E 117C8C84 0390887D

QsV_y is
066F5A57 B6B52B0D F0B3BC9C
DA64E037 F47EF3EB 71959056 CD2E7121 3FD8EDEE 549E2098

deU is
00F7C6B3 BE198B33 AC66FDAA
529278F6 D9CF9226 954DCF7B 4B334AF6 2E37C242 91F0E5A3

QeU_x is
06826AD1 C80EC52B A5ED422E

```
        BCEB4E1A C9BF4815 9213BCF0 1EECB4CA 8ECC2147 8F2E4E62


QeU_y is
                                    0205EA96 61435B98 AF972801
        24824B4E AE66D297 A45D89C5 541576B0 25AF34EF 021AF04B




------------------------------------------------------------
no Key Confirmation
Z is
                                    0091A6BD 5E5C5EF6 48C34B14
        72E6F2F9 C80D1D85 EE2DE0BD E5361921 AA34D915 87A145EF


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                            2F2E1D30 2C05BF13 F1C42B58 51014C1A
        C2BE4688 9CC2CE45 7C7551BE CAF032B1 36190DA8 0067C50C
        304821CA B250B211 61023468 A6BD7AA6 FCC27650 3D5A9E7D


KeyData is
                            2F2E1D30 2C05BF13 F1C42B58 51014C1A
        C2BE4688 9CC2CE45 7C7551BE CAF032B1 36190DA8 0067C50C
        304821CA B250B211 61023468 A6BD7AA6 FCC27650 3D5A9E7D




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
                                    0091A6BD 5E5C5EF6 48C34B14
        72E6F2F9 C80D1D85 EE2DE0BD E5361921 AA34D915 87A145EF


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536
```

```
DerivedKeyMaterial is
                                                2F2E1D30 2C05BF13
        F1C42B58 51014C1A C2BE4688 9CC2CE45 7C7551BE CAF032B1
        36190DA8 0067C50C 304821CA B250B211 61023468 A6BD7AA6
        FCC27650 3D5A9E7D 9F544E00 1017C432 04FCADE7 772288F3


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        06826AD1 C80EC52B A5ED422E BCEB4E1A C9BF4815 9213BCF0
        1EECB4CA 8ECC2147 8F2E4E62 0205EA96 61435B98 AF972801
        24824B4E AE66D297 A45D89C5 541576B0 25AF34EF 021AF04B


MacKey is
                         2F2E1D30 2C05BF13 F1C42B58 51014C1A


Mtag is
                                                F312F183 ECB0F8E7
        ABDFF0DD DB2BB90D 0BA61A0C 7E381599 2805C0CB E4F69FFD


KeyData is
                         C2BE4688 9CC2CE45 7C7551BE CAF032B1
        36190DA8 0067C50C 304821CA B250B211 61023468 A6BD7AA6
        FCC27650 3D5A9E7D 9F544E00 1017C432 04FCADE7 772288F3




StaticUnifiedCDH(K-283)
-------------------------------------------------------------
dsU is
                                    00A350DC 8CCD3420 3183B8D1
        D6F82F0D DC124FE0 593BA2D5 6C59A2A7 BC855CCE 138980DD


QsU_x is
                                    04F651A1 98D31C6F 0B696198
        D914ECEB 11EE20E5 02A8FA3D D509E65B 6B62883F 5399795C


QsU_y is
                                    047973CA 65BBC644 5E11AB4F
        3D6E545D 76770638 398704BE 8544C515 2A2BB3A7 9F602C1B
```

```
dsV is
                                  00379763 1D9722EE C1814DF2
        802BE5D3 FC4EC4E6 E9F4D77A 3BA8E7C5 D3BFF06A BDE926D4


QsV_x is
                                  04AF7AA0 A3A68875 7493840D
        8EEA50C7 65BCA48D 2EC1F731 A2652064 9618E489 2B8CE7CE


QsV_y is
                                  0780C996 9588635C 42F6046D
        D3CC08AF 13E9FB71 16DAA463 1BA5AAFE 0EC2FEFB 2D69BA8C




------------------------------------------------------------
no Key Confirmation
NonceU is
                                  01570933 A3C886AA 674F4D0B
        65B0CADE 72A3CE5C 4074DC8F 3ECCDC2E 684766D3 968328D3


Z is
                                  06B34DC1 AE3C6416 50DB164E
        72757452 16F12605 D5560273 D61CDA05 E1DADE57 E4105A6A


OtherInfo is
                             1234 56789ABC DEF0414C 49434531
        32331B01 01570933 A3C886AA 674F4D0B 65B0CADE 72A3CE5C
        4074DC8F 3ECCDC2E 684766D3 968328D3 424F4242 59343536


DerivedKeyMaterial is
                          36C370CA 31A2DDB6 657E7946 A15BC0E1
        590940FC AC9066C1 DEF8B8C5 1BA2FA53 8BDD4A60 39820BCF
        66D6054A 0252F4B3 D5562A5A F09E6802 C6B25EF4 3438DCE9


KeyData is
                          36C370CA 31A2DDB6 657E7946 A15BC0E1
        590940FC AC9066C1 DEF8B8C5 1BA2FA53 8BDD4A60 39820BCF
```

66D6054A 0252F4B3 D5562A5A F09E6802 C6B25EF4 3438DCE9

Scheme Initiator, Key Confirmation Provider: U to V
NonceU is
01570933 A3C886AA 674F4D0B
65B0CADE 72A3CE5C 4074DC8F 3ECCDC2E 684766D3 968328D3

NonceV is
01F3FB9F F8F29DC3 BB168575
6BDE84A9 B5E44C5E EA232DEA 928500EB 27C54A18 E94E8C0A

Z is
06B34DC1 AE3C6416 50DB164E
72757452 16F12605 D5560273 D61CDA05 E1DADE57 E4105A6A

OtherInfo is
1234 56789ABC DEF0414C 49434531
32331B01 01570933 A3C886AA 674F4D0B 65B0CADE 72A3CE5C
4074DC8F 3ECCDC2E 684766D3 968328D3 424F4242 59343536

DerivedKeyMaterial is
36C370CA 31A2DDB6
657E7946 A15BC0E1 590940FC AC9066C1 DEF8B8C5 1BA2FA53
8BDD4A60 39820BCF 66D6054A 0252F4B3 D5562A5A F09E6802
C6B25EF4 3438DCE9 45C2A191 059CA379 D3E9BDA7 858C7AC0

MacData is
4B435F31 5F55414C 49434542 4F424259
01570933 A3C886AA 674F4D0B 65B0CADE 72A3CE5C 4074DC8F
3ECCDC2E 684766D3 968328D3 01F3FB9F F8F29DC3 BB168575
6BDE84A9 B5E44C5E EA232DEA 928500EB 27C54A18 E94E8C0A

MacKey is
36C370CA 31A2DDB6 657E7946 A15BC0E1

Mtag is
                                                  164AB657 26BA18C8
        151615AB D9C6150C 6409134D B5E0F553 4AC12761 93E53D98

KeyData is
                          590940FC AC9066C1 DEF8B8C5 1BA2FA53
        8BDD4A60 39820BCF 66D6054A 0252F4B3 D5562A5A F09E6802
        C6B25EF4 3438DCE9 45C2A191 059CA379 D3E9BDA7 858C7AC0

Scheme Responder, Key Confirmation Provider: V to U
NonceV is
                                    01F3FB9F F8F29DC3 BB168575
        6BDE84A9 B5E44C5E EA232DEA 928500EB 27C54A18 E94E8C0A

NonceU is
                                    01570933 A3C886AA 674F4D0B
        65B0CADE 72A3CE5C 4074DC8F 3ECCDC2E 684766D3 968328D3

Z is
                                    06B34DC1 AE3C6416 50DB164E
        72757452 16F12605 D5560273 D61CDA05 E1DADE57 E4105A6A

OtherInfo is
                               1234 56789ABC DEF0414C 49434531
        32331B01 01570933 A3C886AA 674F4D0B 65B0CADE 72A3CE5C
        4074DC8F 3ECCDC2E 684766D3 968328D3 424F4242 59343536

DerivedKeyMaterial is
                                                  36C370CA 31A2DDB6
        657E7946 A15BC0E1 590940FC AC9066C1 DEF8B8C5 1BA2FA53
        8BDD4A60 39820BCF 66D6054A 0252F4B3 D5562A5A F09E6802
        C6B25EF4 3438DCE9 45C2A191 059CA379 D3E9BDA7 858C7AC0

MacData is
                                                        4B435F31
        5F56424F 42425941 4C494345 01570933 A3C886AA 674F4D0B

```
        65B0CADE 72A3CE5C 4074DC8F 3ECCDC2E 684766D3 968328D3


MacKey is
                         36C370CA 31A2DDB6 657E7946 A15BC0E1


Mtag is
                                             9C6D9483 4E296AED
        CAFE23F3 2845CE90 387C891A FD13AC22 89096BA5 38EF4602


KeyData is
                         590940FC AC9066C1 DEF8B8C5 1BA2FA53
        8BDD4A60 39820BCF 66D6054A 0252F4B3 D5562A5A F09E6802
        C6B25EF4 3438DCE9 45C2A191 059CA379 D3E9BDA7 858C7AC0




-------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
NonceU is
                                  01570933 A3C886AA 674F4D0B
        65B0CADE 72A3CE5C 4074DC8F 3ECCDC2E 684766D3 968328D3


NonceV is
                                  01F3FB9F F8F29DC3 BB168575
        6BDE84A9 B5E44C5E EA232DEA 928500EB 27C54A18 E94E8C0A


Z is
                                  06B34DC1 AE3C6416 50DB164E
        72757452 16F12605 D5560273 D61CDA05 E1DADE57 E4105A6A


OtherInfo is
                             1234 56789ABC DEF0414C 49434531
        32331B01 01570933 A3C886AA 674F4D0B 65B0CADE 72A3CE5C
        4074DC8F 3ECCDC2E 684766D3 968328D3 424F4242 59343536


DerivedKeyMaterial is
                                             36C370CA 31A2DDB6
```

```
        657E7946 A15BC0E1 590940FC AC9066C1 DEF8B8C5 1BA2FA53
        8BDD4A60 39820BCF 66D6054A 0252F4B3 D5562A5A F09E6802
        C6B25EF4 3438DCE9 45C2A191 059CA379 D3E9BDA7 858C7AC0


U2V
----------------
MacData is
                         4B435F32 5F55414C 49434542 4F424259
        01570933 A3C886AA 674F4D0B 65B0CADE 72A3CE5C 4074DC8F
        3ECCDC2E 684766D3 968328D3 01F3FB9F F8F29DC3 BB168575
        6BDE84A9 B5E44C5E EA232DEA 928500EB 27C54A18 E94E8C0A


MacKey is
                         36C370CA 31A2DDB6 657E7946 A15BC0E1


Mtag is
                                           4B5196F9 126978B6
        271900AA C87BED81 D571D2BD B6A9D456 6C47B9DD D2AB88DD


V2U
----------------
MacData is
                         4B435F32 5F56424F 42425941 4C494345
        01F3FB9F F8F29DC3 BB168575 6BDE84A9 B5E44C5E EA232DEA
        928500EB 27C54A18 E94E8C0A 01570933 A3C886AA 674F4D0B
        65B0CADE 72A3CE5C 4074DC8F 3ECCDC2E 684766D3 968328D3


MacKey is
                         36C370CA 31A2DDB6 657E7946 A15BC0E1


Mtag is
                                           550D6DD8 19A922AD
        40A486F6 38E4B08A 2C0FEEC8 53A3DA94 27057164 3F738656


KeyData is
                         590940FC AC9066C1 DEF8B8C5 1BA2FA53
        8BDD4A60 39820BCF 66D6054A 0252F4B3 D5562A5A F09E6802
        C6B25EF4 3438DCE9 45C2A191 059CA379 D3E9BDA7 858C7AC0
```

```
FullUnifiedCDH(B-283)
-------------------------------------------------------------
dsU is
                                    01452CBF 0E59234E 44CD0835
        4BDEDDDF 60C872F5 4000F338 C074ED44 4E77221A 5D3CE67C


QsU_x is
                                    010F3DC2 488AF9B5 E9367F5C
        E167A621 74312B54 B93F268F 32F276CE B5B2CBFF E51E061F


QsU_y is
                                    02C8ADAF A9D53CB7 B9A80EE1
        50AC705E E2DFADD8 EA305552 1A09869C DB435EE4 BE9FFCA2


dsV is
                                    01116CD6 7A956F4E F9A45B19
        E3FD1DBE B9E494FF 144B3700 A18F5C5F 7F9061A8 7B7BEE70


QsV_x is
                                    012485D1 6088E31C 1B72D53D
        04F72D0D 17519BBD 81D1B494 5660F803 26BA2B2E 9BAF8552


QsV_y is
                                    047F9EA0 285DB578 9BC07A06
        C642D88B 814A5EB2 8E9186E3 52ECC756 5A1D56EE 674F6AF2


deU is
                                    02AFE9DD EA4D9402 C3E2D956
        23B26E03 8A823832 F56D943A D7875566 B829216F C3A470DA


QeU_x is
                                    01D5AA1D 35311907 3EF0FDA3
        E4AC006E 5E02866D 3ADCB3AD 0B9C3275 CCF46E62 3C597F92


QeU_y is
                                    00E0DE25 B45F7BCA E88684B9
```

```
        B127AF63 0E642495 146754F1 01114257 0BBAFAE2 0D81D134


deV is
                                 02547629 7E428505 A6D540D0
        568082A7 AFA287EF 7A565DCE 9828B0D6 33CE2839 9A63673A


QeV_x is
                                 02E0E382 C75A0088 65DBC60D
        37EB00C6 A79A5133 2B98AB8D 05E60CC5 4C9EBC87 2696AA40


QeV_y is
                                 05C450B4 F0D8C8F6 34D55E6E
        FEF79CD5 9C37F434 9FA888E3 0CA21B35 39141B5F 0592C7ED




------------------------------------------------------------
no Key Confirmation
Zs is
                                 063EC199 AF67A235 AEDC7720
        446E4FD8 66CB8C32 481D50CF 9B523E56 35BA61D7 47D33216


Ze is
                                 06E01FB3 8CC2E5B2 D85FB5C7
        ACE9055D 936CA32F 3F7087FC E7C00F85 A47D72B3 4C4F1911


Z is
        06E01FB3 8CC2E5B2 D85FB5C7 ACE9055D 936CA32F 3F7087FC
        E7C00F85 A47D72B3 4C4F1911 063EC199 AF67A235 AEDC7720
        446E4FD8 66CB8C32 481D50CF 9B523E56 35BA61D7 47D33216


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                           C2385897 C36C8CD9 CE697C28 FC92E188
        C7AB6805 A244A5ED 78FE143E 0E0FD6BD AEB62451 F311E2D1
        29D3DBD2 C776DF07 27F9BB6B 849EFB46 B468DE8A 5F9936AA
```

KeyData is
                        C2385897 C36C8CD9 CE697C28 FC92E188
        C7AB6805 A244A5ED 78FE143E 0E0FD6BD AEB62451 F311E2D1
        29D3DBD2 C776DF07 27F9BB6B 849EFB46 B468DE8A 5F9936AA

Scheme Initiator, Key Confirmation Provider: U to V
Zs is
                                 063EC199 AF67A235 AEDC7720
        446E4FD8 66CB8C32 481D50CF 9B523E56 35BA61D7 47D33216

Ze is
                                 06E01FB3 8CC2E5B2 D85FB5C7
        ACE9055D 936CA32F 3F7087FC E7C00F85 A47D72B3 4C4F1911

Z is
        06E01FB3 8CC2E5B2 D85FB5C7 ACE9055D 936CA32F 3F7087FC
        E7C00F85 A47D72B3 4C4F1911 063EC199 AF67A235 AEDC7720
        446E4FD8 66CB8C32 481D50CF 9B523E56 35BA61D7 47D33216

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                                              C2385897 C36C8CD9
        CE697C28 FC92E188 C7AB6805 A244A5ED 78FE143E 0E0FD6BD
        AEB62451 F311E2D1 29D3DBD2 C776DF07 27F9BB6B 849EFB46
        B468DE8A 5F9936AA DB0BA70E 2099F359 30DE4CE5 6746130A

MacData is
                        4B435F31 5F55414C 49434542 4F424259
        01D5AA1D 35311907 3EF0FDA3 E4AC006E 5E02866D 3ADCB3AD
        0B9C3275 CCF46E62 3C597F92 00E0DE25 B45F7BCA E88684B9
        B127AF63 0E642495 146754F1 01114257 0BBAFAE2 0D81D134
        02E0E382 C75A0088 65DBC60D 37EB00C6 A79A5133 2B98AB8D
        05E60CC5 4C9EBC87 2696AA40 05C450B4 F0D8C8F6 34D55E6E

FEF79CD5 9C37F434 9FA888E3 0CA21B35 39141B5F 0592C7ED

MacKey is
C2385897 C36C8CD9 CE697C28 FC92E188

Mtag is
D55B7EFA D67A36ED
1B2F6316 6B9F1D72 ACC35900 384A58F7 0B99702A 2E6F9166

KeyData is
C7AB6805 A244A5ED 78FE143E 0E0FD6BD
AEB62451 F311E2D1 29D3DBD2 C776DF07 27F9BB6B 849EFB46
B468DE8A 5F9936AA DB0BA70E 2099F359 30DE4CE5 6746130A

Scheme Responder, Key Confirmation Provider: V to U
Zs is
063EC199 AF67A235 AEDC7720
446E4FD8 66CB8C32 481D50CF 9B523E56 35BA61D7 47D33216

Ze is
06E01FB3 8CC2E5B2 D85FB5C7
ACE9055D 936CA32F 3F7087FC E7C00F85 A47D72B3 4C4F1911

Z is
06E01FB3 8CC2E5B2 D85FB5C7 ACE9055D 936CA32F 3F7087FC
E7C00F85 A47D72B3 4C4F1911 063EC199 AF67A235 AEDC7720
446E4FD8 66CB8C32 481D50CF 9B523E56 35BA61D7 47D33216

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
C2385897 C36C8CD9
CE697C28 FC92E188 C7AB6805 A244A5ED 78FE143E 0E0FD6BD
AEB62451 F311E2D1 29D3DBD2 C776DF07 27F9BB6B 849EFB46

```
        B468DE8A 5F9936AA DB0BA70E 2099F359 30DE4CE5 6746130A


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        02E0E382 C75A0088 65DBC60D 37EB00C6 A79A5133 2B98AB8D
        05E60CC5 4C9EBC87 2696AA40 05C450B4 F0D8C8F6 34D55E6E
        FEF79CD5 9C37F434 9FA888E3 0CA21B35 39141B5F 0592C7ED
        01D5AA1D 35311907 3EF0FDA3 E4AC006E 5E02866D 3ADCB3AD
        0B9C3275 CCF46E62 3C597F92 00E0DE25 B45F7BCA E88684B9
        B127AF63 0E642495 146754F1 01114257 0BBAFAE2 0D81D134


MacKey is
                         C2385897 C36C8CD9 CE697C28 FC92E188


Mtag is
                                            5A6C318A 6F8A1851
        08AF8C49 251E8D6B 88EF78E1 79A25F08 29B04BCB F19ECA56


KeyData is
                         C7AB6805 A244A5ED 78FE143E 0E0FD6BD
        AEB62451 F311E2D1 29D3DBD2 C776DF07 27F9BB6B 849EFB46
        B468DE8A 5F9936AA DB0BA70E 2099F359 30DE4CE5 6746130A




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
Zs is
                                   063EC199 AF67A235 AEDC7720
        446E4FD8 66CB8C32 481D50CF 9B523E56 35BA61D7 47D33216


Ze is
                                   06E01FB3 8CC2E5B2 D85FB5C7
        ACE9055D 936CA32F 3F7087FC E7C00F85 A47D72B3 4C4F1911


Z is
        06E01FB3 8CC2E5B2 D85FB5C7 ACE9055D 936CA32F 3F7087FC
        E7C00F85 A47D72B3 4C4F1911 063EC199 AF67A235 AEDC7720
        446E4FD8 66CB8C32 481D50CF 9B523E56 35BA61D7 47D33216
```

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                 C2385897 C36C8CD9
        CE697C28 FC92E188 C7AB6805 A244A5ED 78FE143E 0E0FD6BD
        AEB62451 F311E2D1 29D3DBD2 C776DF07 27F9BB6B 849EFB46
        B468DE8A 5F9936AA DB0BA70E 2099F359 30DE4CE5 6746130A


U2V
----------------
MacData is
                         4B435F32 5F55414C 49434542 4F424259
        01D5AA1D 35311907 3EF0FDA3 E4AC006E 5E02866D 3ADCB3AD
        0B9C3275 CCF46E62 3C597F92 00E0DE25 B45F7BCA E88684B9
        B127AF63 0E642495 146754F1 01114257 0BBAFAE2 0D81D134
        02E0E382 C75A0088 65DBC60D 37EB00C6 A79A5133 2B98AB8D
        05E60CC5 4C9EBC87 2696AA40 05C450B4 F0D8C8F6 34D55E6E
        FEF79CD5 9C37F434 9FA888E3 0CA21B35 39141B5F 0592C7ED


MacKey is
                         C2385897 C36C8CD9 CE697C28 FC92E188


Mtag is
                                                 40F73DA5 598F4452
        FD013484 70D66AE5 55152AEC 2069A84F 3957CAD8 311ED3F9


V2U
----------------
MacData is
                         4B435F32 5F56424F 42425941 4C494345
        02E0E382 C75A0088 65DBC60D 37EB00C6 A79A5133 2B98AB8D
        05E60CC5 4C9EBC87 2696AA40 05C450B4 F0D8C8F6 34D55E6E
        FEF79CD5 9C37F434 9FA888E3 0CA21B35 39141B5F 0592C7ED
        01D5AA1D 35311907 3EF0FDA3 E4AC006E 5E02866D 3ADCB3AD
        0B9C3275 CCF46E62 3C597F92 00E0DE25 B45F7BCA E88684B9
        B127AF63 0E642495 146754F1 01114257 0BBAFAE2 0D81D134
```

```
MacKey is
                        C2385897 C36C8CD9 CE697C28 FC92E188


Mtag is
                                          391F7FFC 76A1261C
        EBB88589 026CF58F 7CEAE584 186110EA D2DF06CB 9567F708


KeyData is
                        C7AB6805 A244A5ED 78FE143E 0E0FD6BD
        AEB62451 F311E2D1 29D3DBD2 C776DF07 27F9BB6B 849EFB46
        B468DE8A 5F9936AA DB0BA70E 2099F359 30DE4CE5 6746130A




FullMQV(B-283)
-------------------------------------------------------------
dsU is
                                  01452CBF 0E59234E 44CD0835
        4BDEDDDF 60C872F5 4000F338 C074ED44 4E77221A 5D3CE67C


QsU_x is
                                  010F3DC2 488AF9B5 E9367F5C
        E167A621 74312B54 B93F268F 32F276CE B5B2CBFF E51E061F


QsU_y is
                                  02C8ADAF A9D53CB7 B9A80EE1
        50AC705E E2DFADD8 EA305552 1A09869C DB435EE4 BE9FFCA2


dsV is
                                  01116CD6 7A956F4E F9A45B19
        E3FD1DBE B9E494FF 144B3700 A18F5C5F 7F9061A8 7B7BEE70


QsV_x is
                                  012485D1 6088E31C 1B72D53D
        04F72D0D 17519BBD 81D1B494 5660F803 26BA2B2E 9BAF8552


QsV_y is
                                  047F9EA0 285DB578 9BC07A06
```

```
        C642D88B 814A5EB2 8E9186E3 52ECC756 5A1D56EE 674F6AF2


deU is
                                   02AFE9DD EA4D9402 C3E2D956
        23B26E03 8A823832 F56D943A D7875566 B829216F C3A470DA


QeU_x is
                                   01D5AA1D 35311907 3EF0FDA3
        E4AC006E 5E02866D 3ADCB3AD 0B9C3275 CCF46E62 3C597F92


QeU_y is
                                   00E0DE25 B45F7BCA E88684B9
        B127AF63 0E642495 146754F1 01114257 0BBAFAE2 0D81D134


deV is
                                   02547629 7E428505 A6D540D0
        568082A7 AFA287EF 7A565DCE 9828B0D6 33CE2839 9A63673A


QeV_x is
                                   02E0E382 C75A0088 65DBC60D
        37EB00C6 A79A5133 2B98AB8D 05E60CC5 4C9EBC87 2696AA40


QeV_y is
                                   05C450B4 F0D8C8F6 34D55E6E
        FEF79CD5 9C37F434 9FA888E3 0CA21B35 39141B5F 0592C7ED




------------------------------------------------------------
no Key Confirmation
Z is
                                   012A48E8 3F71807D E52B98FE
        6BDA5FBB C43331CC 91B8ACCB 25D72BC2 1E3204DD 65057463


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536
```

```
DerivedKeyMaterial is
                          5E1E7336 C7E15EFE 2C6CD0BE D0AB6635
        6B53E67A 2C0AFD0E 0B8C5C08 5E2503C9 F6A31F44 EF5BA99D
        C48F46FE F45B0293 8432F9FB 9BA90532 5444523C E91FBC6E


KeyData is
                          5E1E7336 C7E15EFE 2C6CD0BE D0AB6635
        6B53E67A 2C0AFD0E 0B8C5C08 5E2503C9 F6A31F44 EF5BA99D
        C48F46FE F45B0293 8432F9FB 9BA90532 5444523C E91FBC6E




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Z is
                                    012A48E8 3F71807D E52B98FE
        6BDA5FBB C43331CC 91B8ACCB 25D72BC2 1E3204DD 65057463


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                5E1E7336 C7E15EFE
        2C6CD0BE D0AB6635 6B53E67A 2C0AFD0E 0B8C5C08 5E2503C9
        F6A31F44 EF5BA99D C48F46FE F45B0293 8432F9FB 9BA90532
        5444523C E91FBC6E 0932803C 63856F6E 7AA07973 E3EAC97E


MacData is
                          4B435F31 5F55414C 49434542 4F424259
        01D5AA1D 35311907 3EF0FDA3 E4AC006E 5E02866D 3ADCB3AD
        0B9C3275 CCF46E62 3C597F92 00E0DE25 B45F7BCA E88684B9
        B127AF63 0E642495 146754F1 01114257 0BBAFAE2 0D81D134
        02E0E382 C75A0088 65DBC60D 37EB00C6 A79A5133 2B98AB8D
        05E60CC5 4C9EBC87 2696AA40 05C450B4 F0D8C8F6 34D55E6E
        FEF79CD5 9C37F434 9FA888E3 0CA21B35 39141B5F 0592C7ED


MacKey is
                          5E1E7336 C7E15EFE 2C6CD0BE D0AB6635
```

Mtag is
                                                67164C2D 2A1841D7
        81850E83 A51CDD4E CA61345C 88F51487 32B084F5 DE2E4BA8

KeyData is
                            6B53E67A 2C0AFD0E 0B8C5C08 5E2503C9
        F6A31F44 EF5BA99D C48F46FE F45B0293 8432F9FB 9BA90532
        5444523C E91FBC6E 0932803C 63856F6E 7AA07973 E3EAC97E

Scheme Responder, Key Confirmation Provider: V to U
Z is
                                    012A48E8 3F71807D E52B98FE
        6BDA5FBB C43331CC 91B8ACCB 25D72BC2 1E3204DD 65057463

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                                                5E1E7336 C7E15EFE
        2C6CD0BE D0AB6635 6B53E67A 2C0AFD0E 0B8C5C08 5E2503C9
        F6A31F44 EF5BA99D C48F46FE F45B0293 8432F9FB 9BA90532
        5444523C E91FBC6E 0932803C 63856F6E 7AA07973 E3EAC97E

MacData is
                            4B435F31 5F56424F 42425941 4C494345
        02E0E382 C75A0088 65DBC60D 37EB00C6 A79A5133 2B98AB8D
        05E60CC5 4C9EBC87 2696AA40 05C450B4 F0D8C8F6 34D55E6E
        FEF79CD5 9C37F434 9FA888E3 0CA21B35 39141B5F 0592C7ED
        01D5AA1D 35311907 3EF0FDA3 E4AC006E 5E02866D 3ADCB3AD
        0B9C3275 CCF46E62 3C597F92 00E0DE25 B45F7BCA E88684B9
        B127AF63 0E642495 146754F1 01114257 0BBAFAE2 0D81D134

MacKey is
                            5E1E7336 C7E15EFE 2C6CD0BE D0AB6635

Mtag is

```
                                                D46E0D80 9C7BB7B1
        33CB4560 92DFD92C 8BB08FC7 4EEB76B9 D6831D7A 18E07FE5


KeyData is
                         6B53E67A 2C0AFD0E 0B8C5C08 5E2503C9
        F6A31F44 EF5BA99D C48F46FE F45B0293 8432F9FB 9BA90532
        5444523C E91FBC6E 0932803C 63856F6E 7AA07973 E3EAC97E




------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
Z is
                                    012A48E8 3F71807D E52B98FE
        6BDA5FBB C43331CC 91B8ACCB 25D72BC2 1E3204DD 65057463


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                5E1E7336 C7E15EFE
        2C6CD0BE D0AB6635 6B53E67A 2C0AFD0E 0B8C5C08 5E2503C9
        F6A31F44 EF5BA99D C48F46FE F45B0293 8432F9FB 9BA90532
        5444523C E91FBC6E 0932803C 63856F6E 7AA07973 E3EAC97E


U2V
----------------
MacData is
                         4B435F32 5F55414C 49434542 4F424259
        01D5AA1D 35311907 3EF0FDA3 E4AC006E 5E02866D 3ADCB3AD
        0B9C3275 CCF46E62 3C597F92 00E0DE25 B45F7BCA E88684B9
        B127AF63 0E642495 146754F1 01114257 0BBAFAE2 0D81D134
        02E0E382 C75A0088 65DBC60D 37EB00C6 A79A5133 2B98AB8D
        05E60CC5 4C9EBC87 2696AA40 05C450B4 F0D8C8F6 34D55E6E
        FEF79CD5 9C37F434 9FA888E3 0CA21B35 39141B5F 0592C7ED


MacKey is
                         5E1E7336 C7E15EFE 2C6CD0BE D0AB6635
```

```
Mtag is
                                                 72F0D670 FB5FA804
        BF088C56 1ADAE9D5 6D3006AB EC57FDCF 1D5FE65B 35A03611


V2U
----------------
MacData is
                         4B435F32 5F56424F 42425941 4C494345
        02E0E382 C75A0088 65DBC60D 37EB00C6 A79A5133 2B98AB8D
        05E60CC5 4C9EBC87 2696AA40 05C450B4 F0D8C8F6 34D55E6E
        FEF79CD5 9C37F434 9FA888E3 0CA21B35 39141B5F 0592C7ED
        01D5AA1D 35311907 3EF0FDA3 E4AC006E 5E02866D 3ADCB3AD
        0B9C3275 CCF46E62 3C597F92 00E0DE25 B45F7BCA E88684B9
        B127AF63 0E642495 146754F1 01114257 0BBAFAE2 0D81D134


MacKey is
                         5E1E7336 C7E15EFE 2C6CD0BE D0AB6635


Mtag is
                                                 CD332035 4F0F7712
        91313CB9 0D4CB293 067F2F4F F82ADE00 109C94B7 166D1A65


KeyData is
                         6B53E67A 2C0AFD0E 0B8C5C08 5E2503C9
        F6A31F44 EF5BA99D C48F46FE F45B0293 8432F9FB 9BA90532
        5444523C E91FBC6E 0932803C 63856F6E 7AA07973 E3EAC97E




EphemeralUnifiedCDH(B-283)
------------------------------------------------------------
deU is
                                    02AFE9DD EA4D9402 C3E2D956
        23B26E03 8A823832 F56D943A D7875566 B829216F C3A470DA


QeU_x is
                                    01D5AA1D 35311907 3EF0FDA3
        E4AC006E 5E02866D 3ADCB3AD 0B9C3275 CCF46E62 3C597F92
```

```
QeU_y is
                                00E0DE25 B45F7BCA E88684B9
        B127AF63 0E642495 146754F1 01114257 0BBAFAE2 0D81D134


deV is
                                02547629 7E428505 A6D540D0
        568082A7 AFA287EF 7A565DCE 9828B0D6 33CE2839 9A63673A


QeV_x is
                                02E0E382 C75A0088 65DBC60D
        37EB00C6 A79A5133 2B98AB8D 05E60CC5 4C9EBC87 2696AA40


QeV_y is
                                05C450B4 F0D8C8F6 34D55E6E
        FEF79CD5 9C37F434 9FA888E3 0CA21B35 39141B5F 0592C7ED




------------------------------------------------------------
no Key Confirmation
Z is
                                06E01FB3 8CC2E5B2 D85FB5C7
        ACE9055D 936CA32F 3F7087FC E7C00F85 A47D72B3 4C4F1911


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                            891C76BC 5AA31DC2 C8953424 2E0A85A3
        F24B22B5 B6A2E70C 3ECA0971 7941EE6E 14AA39FB 611B8AEC
        DC23B30C 02873A45 7966C625 4EF9ECBE 0CD15192 EF26225E


KeyData is
                            891C76BC 5AA31DC2 C8953424 2E0A85A3
        F24B22B5 B6A2E70C 3ECA0971 7941EE6E 14AA39FB 611B8AEC
        DC23B30C 02873A45 7966C625 4EF9ECBE 0CD15192 EF26225E
```

OnePassUnifiedCDH(B-283)
---
dsU is
01452CBF 0E59234E 44CD0835
4BDEDDDF 60C872F5 4000F338 C074ED44 4E77221A 5D3CE67C

QsU_x is
010F3DC2 488AF9B5 E9367F5C
E167A621 74312B54 B93F268F 32F276CE B5B2CBFF E51E061F

QsU_y is
02C8ADAF A9D53CB7 B9A80EE1
50AC705E E2DFADD8 EA305552 1A09869C DB435EE4 BE9FFCA2

dsV is
01116CD6 7A956F4E F9A45B19
E3FD1DBE B9E494FF 144B3700 A18F5C5F 7F9061A8 7B7BEE70

QsV_x is
012485D1 6088E31C 1B72D53D
04F72D0D 17519BBD 81D1B494 5660F803 26BA2B2E 9BAF8552

QsV_y is
047F9EA0 285DB578 9BC07A06
C642D88B 814A5EB2 8E9186E3 52ECC756 5A1D56EE 674F6AF2

deU is
02AFE9DD EA4D9402 C3E2D956
23B26E03 8A823832 F56D943A D7875566 B829216F C3A470DA

QeU_x is
01D5AA1D 35311907 3EF0FDA3
E4AC006E 5E02866D 3ADCB3AD 0B9C3275 CCF46E62 3C597F92

QeU_y is
00E0DE25 B45F7BCA E88684B9

B127AF63 0E642495 146754F1 01114257 0BBAFAE2 0D81D134

---

no Key Confirmation
Zs is
063EC199 AF67A235 AEDC7720
446E4FD8 66CB8C32 481D50CF 9B523E56 35BA61D7 47D33216

Ze is
055FCC43 81AEA086 60FF8F01
69C57B67 2C3ABDE9 FA028135 C1EA1195 20C07680 DA894372

Z is
055FCC43 81AEA086 60FF8F01 69C57B67 2C3ABDE9 FA028135
C1EA1195 20C07680 DA894372 063EC199 AF67A235 AEDC7720
446E4FD8 66CB8C32 481D50CF 9B523E56 35BA61D7 47D33216

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
90DB59EB F9AB2D31 9DB4B924 6229822B
82F6ACE1 C1839AAA 61F9D948 01BE1F55 5C34C0BC B8F60D74
6827A0CA CEC0A1A6 24A05D32 3B22C2E4 932B6617 8B3F5EB9

KeyData is
90DB59EB F9AB2D31 9DB4B924 6229822B
82F6ACE1 C1839AAA 61F9D948 01BE1F55 5C34C0BC B8F60D74
6827A0CA CEC0A1A6 24A05D32 3B22C2E4 932B6617 8B3F5EB9

Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
00AB1733 41ED3D3E 49946150
E15831CF 0564D21F CDB76893 F527D5BB 7F5C2F6B C69CE514

```
Zs is
                                063EC199 AF67A235 AEDC7720
        446E4FD8 66CB8C32 481D50CF 9B523E56 35BA61D7 47D33216


Ze is
                                055FCC43 81AEA086 60FF8F01
        69C57B67 2C3ABDE9 FA028135 C1EA1195 20C07680 DA894372


Z is
        055FCC43 81AEA086 60FF8F01 69C57B67 2C3ABDE9 FA028135
        C1EA1195 20C07680 DA894372 063EC199 AF67A235 AEDC7720
        446E4FD8 66CB8C32 481D50CF 9B523E56 35BA61D7 47D33216


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                            90DB59EB F9AB2D31
        9DB4B924 6229822B 82F6ACE1 C1839AAA 61F9D948 01BE1F55
        5C34C0BC B8F60D74 6827A0CA CEC0A1A6 24A05D32 3B22C2E4
        932B6617 8B3F5EB9 7EB209A6 4DBA0DB0 1D725561 A59583C5


MacData is
                                                    4B435F31
        5F55414C 49434542 4F424259 01D5AA1D 35311907 3EF0FDA3
        E4AC006E 5E02866D 3ADCB3AD 0B9C3275 CCF46E62 3C597F92
        00E0DE25 B45F7BCA E88684B9 B127AF63 0E642495 146754F1
        01114257 0BBAFAE2 0D81D134 00AB1733 41ED3D3E 49946150
        E15831CF 0564D21F CDB76893 F527D5BB 7F5C2F6B C69CE514


MacKey is
                        90DB59EB F9AB2D31 9DB4B924 6229822B


Mtag is
                                            162B7EF4 189C767F
        AABF9071 BB86A97C 895D3DC1 169E9B5C D8F0C1F4 986BC6B1
```

KeyData is
                        82F6ACE1 C1839AAA 61F9D948 01BE1F55
        5C34C0BC B8F60D74 6827A0CA CEC0A1A6 24A05D32 3B22C2E4
        932B6617 8B3F5EB9 7EB209A6 4DBA0DB0 1D725561 A59583C5

Scheme Responder, Key Confirmation Provider: V to U
NonceU is
                                00AB1733 41ED3D3E 49946150
        E15831CF 0564D21F CDB76893 F527D5BB 7F5C2F6B C69CE514

Zs is
                                063EC199 AF67A235 AEDC7720
        446E4FD8 66CB8C32 481D50CF 9B523E56 35BA61D7 47D33216

Ze is
                                055FCC43 81AEA086 60FF8F01
        69C57B67 2C3ABDE9 FA028135 C1EA1195 20C07680 DA894372

Z is
        055FCC43 81AEA086 60FF8F01 69C57B67 2C3ABDE9 FA028135
        C1EA1195 20C07680 DA894372 063EC199 AF67A235 AEDC7720
        446E4FD8 66CB8C32 481D50CF 9B523E56 35BA61D7 47D33216

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                                            90DB59EB F9AB2D31
        9DB4B924 6229822B 82F6ACE1 C1839AAA 61F9D948 01BE1F55
        5C34C0BC B8F60D74 6827A0CA CEC0A1A6 24A05D32 3B22C2E4
        932B6617 8B3F5EB9 7EB209A6 4DBA0DB0 1D725561 A59583C5

MacData is
                        4B435F31 5F56424F 42425941 4C494345
        01D5AA1D 35311907 3EF0FDA3 E4AC006E 5E02866D 3ADCB3AD

```
        0B9C3275 CCF46E62 3C597F92 00E0DE25 B45F7BCA E88684B9
        B127AF63 0E642495 146754F1 01114257 0BBAFAE2 0D81D134


MacKey is
                         90DB59EB F9AB2D31 9DB4B924 6229822B


Mtag is
                                           ECA624CD A4098CCC
        12B9FEE1 CA7AC88E 698166F9 C1299093 E17B1929 9EEF78F5


KeyData is
                         82F6ACE1 C1839AAA 61F9D948 01BE1F55
        5C34C0BC B8F60D74 6827A0CA CEC0A1A6 24A05D32 3B22C2E4
        932B6617 8B3F5EB9 7EB209A6 4DBA0DB0 1D725561 A59583C5




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
                                   00AB1733 41ED3D3E 49946150
        E15831CF 0564D21F CDB76893 F527D5BB 7F5C2F6B C69CE514


Zs is
                                   063EC199 AF67A235 AEDC7720
        446E4FD8 66CB8C32 481D50CF 9B523E56 35BA61D7 47D33216


Ze is
                                   055FCC43 81AEA086 60FF8F01
        69C57B67 2C3ABDE9 FA028135 C1EA1195 20C07680 DA894372


Z is
        055FCC43 81AEA086 60FF8F01 69C57B67 2C3ABDE9 FA028135
        C1EA1195 20C07680 DA894372 063EC199 AF67A235 AEDC7720
        446E4FD8 66CB8C32 481D50CF 9B523E56 35BA61D7 47D33216


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536
```

```
DerivedKeyMaterial is
                                                90DB59EB F9AB2D31
        9DB4B924 6229822B 82F6ACE1 C1839AAA 61F9D948 01BE1F55
        5C34C0BC B8F60D74 6827A0CA CEC0A1A6 24A05D32 3B22C2E4
        932B6617 8B3F5EB9 7EB209A6 4DBA0DB0 1D725561 A59583C5


U2V
----------------
MacData is
                                                        4B435F32
        5F55414C 49434542 4F424259 01D5AA1D 35311907 3EF0FDA3
        E4AC006E 5E02866D 3ADCB3AD 0B9C3275 CCF46E62 3C597F92
        00E0DE25 B45F7BCA E88684B9 B127AF63 0E642495 146754F1
        01114257 0BBAFAE2 0D81D134 00AB1733 41ED3D3E 49946150
        E15831CF 0564D21F CDB76893 F527D5BB 7F5C2F6B C69CE514


MacKey is
                        90DB59EB F9AB2D31 9DB4B924 6229822B


Mtag is
                                                6572D13B F7DAE145
        5F923F14 165CB528 D249A295 8C40014D 1B3A26D8 7C3FC3F0


V2U
----------------
MacData is
                                                        4B435F32
        5F56424F 42425941 4C494345 00AB1733 41ED3D3E 49946150
        E15831CF 0564D21F CDB76893 F527D5BB 7F5C2F6B C69CE514
        01D5AA1D 35311907 3EF0FDA3 E4AC006E 5E02866D 3ADCB3AD
        0B9C3275 CCF46E62 3C597F92 00E0DE25 B45F7BCA E88684B9
        B127AF63 0E642495 146754F1 01114257 0BBAFAE2 0D81D134


MacKey is
                        90DB59EB F9AB2D31 9DB4B924 6229822B


Mtag is
                                                DD296F26 27940E90
```

```
        3CC13E1F 9B21946A 938F7CAD 01BBADAE D91912BE 7B94E99F


KeyData is
                         82F6ACE1 C1839AAA 61F9D948 01BE1F55
        5C34C0BC B8F60D74 6827A0CA CEC0A1A6 24A05D32 3B22C2E4
        932B6617 8B3F5EB9 7EB209A6 4DBA0DB0 1D725561 A59583C5




OnePassMQV(B-283)
------------------------------------------------------------
dsU is
                                  01452CBF 0E59234E 44CD0835
        4BDEDDDF 60C872F5 4000F338 C074ED44 4E77221A 5D3CE67C


QsU_x is
                                  010F3DC2 488AF9B5 E9367F5C
        E167A621 74312B54 B93F268F 32F276CE B5B2CBFF E51E061F


QsU_y is
                                  02C8ADAF A9D53CB7 B9A80EE1
        50AC705E E2DFADD8 EA305552 1A09869C DB435EE4 BE9FFCA2


dsV is
                                  01116CD6 7A956F4E F9A45B19
        E3FD1DBE B9E494FF 144B3700 A18F5C5F 7F9061A8 7B7BEE70


QsV_x is
                                  012485D1 6088E31C 1B72D53D
        04F72D0D 17519BBD 81D1B494 5660F803 26BA2B2E 9BAF8552


QsV_y is
                                  047F9EA0 285DB578 9BC07A06
        C642D88B 814A5EB2 8E9186E3 52ECC756 5A1D56EE 674F6AF2


deU is
                                  02AFE9DD EA4D9402 C3E2D956
        23B26E03 8A823832 F56D943A D7875566 B829216F C3A470DA
```

```
QeU_x is
                                    01D5AA1D 35311907 3EF0FDA3
        E4AC006E 5E02866D 3ADCB3AD 0B9C3275 CCF46E62 3C597F92


QeU_y is
                                    00E0DE25 B45F7BCA E88684B9
        B127AF63 0E642495 146754F1 01114257 0BBAFAE2 0D81D134




------------------------------------------------------------
no Key Confirmation
Z is
                                    0387E550 2749B77E 85E1770F
        88CC8B35 8C6EC752 5332AB25 CAE4C785 4DA2BC2F 6A78906E


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                            93B9BF12 B1BA41FF 3D424261 4A22CE33
        94CAB872 7C043931 EDC853EB BB6AE609 08CD9A13 6DE159D3
        BBC7EA31 C84703EE 64186F73 5A2B31E5 81708DE5 60A2FCD0


KeyData is
                            93B9BF12 B1BA41FF 3D424261 4A22CE33
        94CAB872 7C043931 EDC853EB BB6AE609 08CD9A13 6DE159D3
        BBC7EA31 C84703EE 64186F73 5A2B31E5 81708DE5 60A2FCD0




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                                    00AB1733 41ED3D3E 49946150
        E15831CF 0564D21F CDB76893 F527D5BB 7F5C2F6B C69CE514
```

Z is
                                0387E550 2749B77E 85E1770F
        88CC8B35 8C6EC752 5332AB25 CAE4C785 4DA2BC2F 6A78906E

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                                                 93B9BF12 B1BA41FF
        3D424261 4A22CE33 94CAB872 7C043931 EDC853EB BB6AE609
        08CD9A13 6DE159D3 BBC7EA31 C84703EE 64186F73 5A2B31E5
        81708DE5 60A2FCD0 6A6F6173 B79756F0 245DA29C 1B4E4FD7

MacData is
                                                          4B435F31
        5F55414C 49434542 4F424259 01D5AA1D 35311907 3EF0FDA3
        E4AC006E 5E02866D 3ADCB3AD 0B9C3275 CCF46E62 3C597F92
        00E0DE25 B45F7BCA E88684B9 B127AF63 0E642495 146754F1
        01114257 0BBAFAE2 0D81D134 00AB1733 41ED3D3E 49946150
        E15831CF 0564D21F CDB76893 F527D5BB 7F5C2F6B C69CE514

MacKey is
                        93B9BF12 B1BA41FF 3D424261 4A22CE33

Mtag is
                                                 30F94887 6337638B
        28F5B9E6 4BA3FB89 4C00E5FF 7A43960D 8871C265 61F0E398

KeyData is
                        94CAB872 7C043931 EDC853EB BB6AE609
        08CD9A13 6DE159D3 BBC7EA31 C84703EE 64186F73 5A2B31E5
        81708DE5 60A2FCD0 6A6F6173 B79756F0 245DA29C 1B4E4FD7

Scheme Responder, Key Confirmation Provider: V to U
NonceU is
                                00AB1733 41ED3D3E 49946150

```
        E15831CF 0564D21F CDB76893 F527D5BB 7F5C2F6B C69CE514


Z is
                                  0387E550 2749B77E 85E1770F
        88CC8B35 8C6EC752 5332AB25 CAE4C785 4DA2BC2F 6A78906E


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                              93B9BF12 B1BA41FF
        3D424261 4A22CE33 94CAB872 7C043931 EDC853EB BB6AE609
        08CD9A13 6DE159D3 BBC7EA31 C84703EE 64186F73 5A2B31E5
        81708DE5 60A2FCD0 6A6F6173 B79756F0 245DA29C 1B4E4FD7


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        01D5AA1D 35311907 3EF0FDA3 E4AC006E 5E02866D 3ADCB3AD
        0B9C3275 CCF46E62 3C597F92 00E0DE25 B45F7BCA E88684B9
        B127AF63 0E642495 146754F1 01114257 0BBAFAE2 0D81D134


MacKey is
                         93B9BF12 B1BA41FF 3D424261 4A22CE33


Mtag is
                                              7680EE94 AF5FE0E1
        3EB199D7 5C8D1189 C7925E42 13227120 8DF0D906 5D523E4D


KeyData is
                         94CAB872 7C043931 EDC853EB BB6AE609
        08CD9A13 6DE159D3 BBC7EA31 C84703EE 64186F73 5A2B31E5
        81708DE5 60A2FCD0 6A6F6173 B79756F0 245DA29C 1B4E4FD7




-------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
```

```
                                00AB1733 41ED3D3E 49946150
        E15831CF 0564D21F CDB76893 F527D5BB 7F5C2F6B C69CE514


Z is
                                0387E550 2749B77E 85E1770F
        88CC8B35 8C6EC752 5332AB25 CAE4C785 4DA2BC2F 6A78906E


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                 93B9BF12 B1BA41FF
        3D424261 4A22CE33 94CAB872 7C043931 EDC853EB BB6AE609
        08CD9A13 6DE159D3 BBC7EA31 C84703EE 64186F73 5A2B31E5
        81708DE5 60A2FCD0 6A6F6173 B79756F0 245DA29C 1B4E4FD7


U2V
----------------
MacData is
                                                          4B435F32
        5F55414C 49434542 4F424259 01D5AA1D 35311907 3EF0FDA3
        E4AC006E 5E02866D 3ADCB3AD 0B9C3275 CCF46E62 3C597F92
        00E0DE25 B45F7BCA E88684B9 B127AF63 0E642495 146754F1
        01114257 0BBAFAE2 0D81D134 00AB1733 41ED3D3E 49946150
        E15831CF 0564D21F CDB76893 F527D5BB 7F5C2F6B C69CE514


MacKey is
                          93B9BF12 B1BA41FF 3D424261 4A22CE33


Mtag is
                                                 BEBD252F 98818468
        C9C4F3CD 13D55C72 E8EC9F54 8CB2AF7E 4FA0A66C 24A0639B


V2U
----------------
MacData is
                                                          4B435F32
        5F56424F 42425941 4C494345 00AB1733 41ED3D3E 49946150
        E15831CF 0564D21F CDB76893 F527D5BB 7F5C2F6B C69CE514
```

```
        01D5AA1D 35311907 3EF0FDA3 E4AC006E 5E02866D 3ADCB3AD
        0B9C3275 CCF46E62 3C597F92 00E0DE25 B45F7BCA E88684B9
        B127AF63 0E642495 146754F1 01114257 0BBAFAE2 0D81D134


MacKey is
                         93B9BF12 B1BA41FF 3D424261 4A22CE33


Mtag is
                                            4327475D DF47C2DE
        2A25B6A6 B5A22E98 94295F95 19A1EF99 82907C06 85614144


KeyData is
                         94CAB872 7C043931 EDC853EB BB6AE609
        08CD9A13 6DE159D3 BBC7EA31 C84703EE 64186F73 5A2B31E5
        81708DE5 60A2FCD0 6A6F6173 B79756F0 245DA29C 1B4E4FD7




OnePassDiffieHellmanCDH(B-283)
------------------------------------------------------------
dsV is
                                    01116CD6 7A956F4E F9A45B19
        E3FD1DBE B9E494FF 144B3700 A18F5C5F 7F9061A8 7B7BEE70


QsV_x is
                                    012485D1 6088E31C 1B72D53D
        04F72D0D 17519BBD 81D1B494 5660F803 26BA2B2E 9BAF8552


QsV_y is
                                    047F9EA0 285DB578 9BC07A06
        C642D88B 814A5EB2 8E9186E3 52ECC756 5A1D56EE 674F6AF2


deU is
                                    02AFE9DD EA4D9402 C3E2D956
        23B26E03 8A823832 F56D943A D7875566 B829216F C3A470DA


QeU_x is
                                    01D5AA1D 35311907 3EF0FDA3
```

E4AC006E 5E02866D 3ADCB3AD 0B9C3275 CCF46E62 3C597F92

QeU_y is
00E0DE25 B45F7BCA E88684B9
B127AF63 0E642495 146754F1 01114257 0BBAFAE2 0D81D134

---

no Key Confirmation
Z is
055FCC43 81AEA086 60FF8F01
69C57B67 2C3ABDE9 FA028135 C1EA1195 20C07680 DA894372

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
43287BE3 E4FDC000 601926F8 A2A42702
B75F649E B0F267B9 9F0F5899 E5A01425 BFADBF8E 82B1CCAA
8F563CA4 8664DD1C CD6C41A0 F880D180 4FFD614F F1650D38

KeyData is
43287BE3 E4FDC000 601926F8 A2A42702
B75F649E B0F267B9 9F0F5899 E5A01425 BFADBF8E 82B1CCAA
8F563CA4 8664DD1C CD6C41A0 F880D180 4FFD614F F1650D38

Scheme Responder, Key Confirmation Provider: V to U
Z is
055FCC43 81AEA086 60FF8F01
69C57B67 2C3ABDE9 FA028135 C1EA1195 20C07680 DA894372

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

```
DerivedKeyMaterial is
                                                43287BE3 E4FDC000
        601926F8 A2A42702 B75F649E B0F267B9 9F0F5899 E5A01425
        BFADBF8E 82B1CCAA 8F563CA4 8664DD1C CD6C41A0 F880D180
        4FFD614F F1650D38 0754F19D 0A34D52C 34A12662 B110AE49


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        01D5AA1D 35311907 3EF0FDA3 E4AC006E 5E02866D 3ADCB3AD
        0B9C3275 CCF46E62 3C597F92 00E0DE25 B45F7BCA E88684B9
        B127AF63 0E642495 146754F1 01114257 0BBAFAE2 0D81D134


MacKey is
                         43287BE3 E4FDC000 601926F8 A2A42702


Mtag is
                                                11B474FC D749C122
        0D87F8D8 A228D320 F9EAB9BB 5C810911 2B34984B A83D0402


KeyData is
                         B75F649E B0F267B9 9F0F5899 E5A01425
        BFADBF8E 82B1CCAA 8F563CA4 8664DD1C CD6C41A0 F880D180
        4FFD614F F1650D38 0754F19D 0A34D52C 34A12662 B110AE49




StaticUnifiedCDH(B-283)
-------------------------------------------------------------
dsU is
                                    00330A8A B17D3C79 FDCE96E3
        E8D8FB76 629206C9 761E1D0F ACEA7BF3 1242359B 62B3490A


QsU_x is
                                    061899B1 8C49FBFD AAF6F044
        BFF7355B 37253CCF 39CC6EFB 7C784E09 7EAA597C D8538D6A


QsU_y is
                                    027D494A B581429E D39462DC
        9F037A9F 38B705B9 FAA61BEC C8F6268E D3A1F688 811B5400
```

```
dsV is
                                  01265C2B D573D6FD 6AD3F598
        72B6B057 4B52302C CF26D56C 65248148 C7AE93C2 6D8E54DC


QsV_x is
                                  0650BE70 7566707F 958D453C
        A0DDCB3C 2E552237 92931AB2 48942112 2CDB77A3 575F51AA


QsV_y is
                                  040E2423 82B6C00E BEE228AA
        0176CD4E 21B8C49F ED592FEA B3B7942B 9F4D61F7 378CF124




------------------------------------------------------------
no Key Confirmation
NonceU is
                                  00AB1733 41ED3D3E 49946150
        E15831CF 0564D21F CDB76893 F527D5BB 7F5C2F6B C69CE514


Z is
                                  0237202F 203A2EEE CC066E87
        539D78AC 69161DC2 BB36648E CAF0D512 3790CD70 F47AB98B


OtherInfo is
                             1234 56789ABC DEF0414C 49434531
        32331B01 00AB1733 41ED3D3E 49946150 E15831CF 0564D21F
        CDB76893 F527D5BB 7F5C2F6B C69CE514 424F4242 59343536


DerivedKeyMaterial is
                          D2E18A86 2C7745E1 2A0EE481 05D8E985
        F4F1E940 2BC4CE2A 099A39B2 6A1922F9 84F336D6 CE2A39F6
        939B193F 802627C0 3B1732CB 41F3AF5C 3798479F 18BE4662


KeyData is
                          D2E18A86 2C7745E1 2A0EE481 05D8E985
        F4F1E940 2BC4CE2A 099A39B2 6A1922F9 84F336D6 CE2A39F6
```

939B193F 802627C0 3B1732CB 41F3AF5C 3798479F 18BE4662

Scheme Initiator, Key Confirmation Provider: U to V
NonceU is
00AB1733 41ED3D3E 49946150
E15831CF 0564D21F CDB76893 F527D5BB 7F5C2F6B C69CE514

NonceV is
02B79F48 88CC6ADF 9D43EA4B
EB7B9D68 E43B41D3 4CA6B5E0 58557342 62AA50B9 83CF2B16

Z is
0237202F 203A2EEE CC066E87
539D78AC 69161DC2 BB36648E CAF0D512 3790CD70 F47AB98B

OtherInfo is
1234 56789ABC DEF0414C 49434531
32331B01 00AB1733 41ED3D3E 49946150 E15831CF 0564D21F
CDB76893 F527D5BB 7F5C2F6B C69CE514 424F4242 59343536

DerivedKeyMaterial is
D2E18A86 2C7745E1
2A0EE481 05D8E985 F4F1E940 2BC4CE2A 099A39B2 6A1922F9
84F336D6 CE2A39F6 939B193F 802627C0 3B1732CB 41F3AF5C
3798479F 18BE4662 5FA9A838 7AFF5B58 C629937E 8B9136CA

MacData is
4B435F31 5F55414C 49434542 4F424259
00AB1733 41ED3D3E 49946150 E15831CF 0564D21F CDB76893
F527D5BB 7F5C2F6B C69CE514 02B79F48 88CC6ADF 9D43EA4B
EB7B9D68 E43B41D3 4CA6B5E0 58557342 62AA50B9 83CF2B16

MacKey is
D2E18A86 2C7745E1 2A0EE481 05D8E985

Mtag is
                                                74D97F14 EC9DE56D
        8ABE560C E8FD97D4 9C9A8BB7 326941FC 547C5951 B44B0BA9

KeyData is
                          F4F1E940 2BC4CE2A 099A39B2 6A1922F9
        84F336D6 CE2A39F6 939B193F 802627C0 3B1732CB 41F3AF5C
        3798479F 18BE4662 5FA9A838 7AFF5B58 C629937E 8B9136CA

Scheme Responder, Key Confirmation Provider: V to U
NonceV is
                                    02B79F48 88CC6ADF 9D43EA4B
        EB7B9D68 E43B41D3 4CA6B5E0 58557342 62AA50B9 83CF2B16

NonceU is
                                    00AB1733 41ED3D3E 49946150
        E15831CF 0564D21F CDB76893 F527D5BB 7F5C2F6B C69CE514

Z is
                                    0237202F 203A2EEE CC066E87
        539D78AC 69161DC2 BB36648E CAF0D512 3790CD70 F47AB98B

OtherInfo is
                               1234 56789ABC DEF0414C 49434531
        32331B01 00AB1733 41ED3D3E 49946150 E15831CF 0564D21F
        CDB76893 F527D5BB 7F5C2F6B C69CE514 424F4242 59343536

DerivedKeyMaterial is
                                                D2E18A86 2C7745E1
        2A0EE481 05D8E985 F4F1E940 2BC4CE2A 099A39B2 6A1922F9
        84F336D6 CE2A39F6 939B193F 802627C0 3B1732CB 41F3AF5C
        3798479F 18BE4662 5FA9A838 7AFF5B58 C629937E 8B9136CA

MacData is
                                                        4B435F31
        5F56424F 42425941 4C494345 00AB1733 41ED3D3E 49946150

E15831CF 0564D21F CDB76893 F527D5BB 7F5C2F6B C69CE514

MacKey is
D2E18A86 2C7745E1 2A0EE481 05D8E985

Mtag is
B661150B 3BF410C9
34AA3AB8 2C6F45CE C8C7A6CE 3A1580EE F20B903E 5623D839

KeyData is
F4F1E940 2BC4CE2A 099A39B2 6A1922F9
84F336D6 CE2A39F6 939B193F 802627C0 3B1732CB 41F3AF5C
3798479F 18BE4662 5FA9A838 7AFF5B58 C629937E 8B9136CA

Scheme Initiator, Key Confirmation Bilateral
NonceU is
00AB1733 41ED3D3E 49946150
E15831CF 0564D21F CDB76893 F527D5BB 7F5C2F6B C69CE514

NonceV is
02B79F48 88CC6ADF 9D43EA4B
EB7B9D68 E43B41D3 4CA6B5E0 58557342 62AA50B9 83CF2B16

Z is
0237202F 203A2EEE CC066E87
539D78AC 69161DC2 BB36648E CAF0D512 3790CD70 F47AB98B

OtherInfo is
1234 56789ABC DEF0414C 49434531
32331B01 00AB1733 41ED3D3E 49946150 E15831CF 0564D21F
CDB76893 F527D5BB 7F5C2F6B C69CE514 424F4242 59343536

DerivedKeyMaterial is
D2E18A86 2C7745E1

```
        2A0EE481 05D8E985 F4F1E940 2BC4CE2A 099A39B2 6A1922F9
        84F336D6 CE2A39F6 939B193F 802627C0 3B1732CB 41F3AF5C
        3798479F 18BE4662 5FA9A838 7AFF5B58 C629937E 8B9136CA


U2V
----------------
MacData is
                         4B435F32 5F55414C 49434542 4F424259
        00AB1733 41ED3D3E 49946150 E15831CF 0564D21F CDB76893
        F527D5BB 7F5C2F6B C69CE514 02B79F48 88CC6ADF 9D43EA4B
        EB7B9D68 E43B41D3 4CA6B5E0 58557342 62AA50B9 83CF2B16


MacKey is
                         D2E18A86 2C7745E1 2A0EE481 05D8E985


Mtag is
                                           09E39393 50277DE9
        335D7439 5EE03999 53C2F945 02AE5DE3 CC28E712 987E46A3


V2U
----------------
MacData is
                         4B435F32 5F56424F 42425941 4C494345
        02B79F48 88CC6ADF 9D43EA4B EB7B9D68 E43B41D3 4CA6B5E0
        58557342 62AA50B9 83CF2B16 00AB1733 41ED3D3E 49946150
        E15831CF 0564D21F CDB76893 F527D5BB 7F5C2F6B C69CE514


MacKey is
                         D2E18A86 2C7745E1 2A0EE481 05D8E985


Mtag is
                                           4DEE0C73 5A82D797
        428E0B4C 80C89C27 81668D0C 79D97868 C5FCF1FE D9C45DA6


KeyData is
                         F4F1E940 2BC4CE2A 099A39B2 6A1922F9
        84F336D6 CE2A39F6 939B193F 802627C0 3B1732CB 41F3AF5C
        3798479F 18BE4662 5FA9A838 7AFF5B58 C629937E 8B9136CA
```

```
FullUnifiedCDH(K-409)
------------------------------------------------------------
dsU is
                                                        0072A861
        311C6905 1FA44C65 A2153631 F19A443F 6B882C28 F4F9C762
        EF30092B 703809D7 5C0892C2 81BA205C 5D870D63 A769033D


QsU_x is
                                                        0152E7F8
        335C1766 4DA0AE5C 7362B49E 14E68453 21768152 5510421F
        A24F5F07 AB1DF096 79398A1F AABF279D 3C44F214 E96DB92A


QsU_y is
                                                        002E3FEF
        D35E52C0 10EBAAD3 C5DBEAF6 9868E630 7D0DAC71 2C7B736D
        474666F9 8B880A5B 25E3B6BA 10098EA8 8AF8FA0E 3C5F4A8D


dsV is
                                                        0047F7DF
        0EB84625 BFE69F8C 9DE845AF A5A26EDD C41B6B56 47360A53
        71398245 8EA0231A F2DA0BAE FA71EB6C 05E1B7D0 837BBFA1


QsV_x is
                                                        0107C00B
        AB1A1085 9172E54E B34DC8BE 22ECCAF9 08E65F4E B97BF481
        F86C0B15 DB869112 8CABD886 9CDDC529 B48AFF82 819A79D0


QsV_y is
                                                        01321631
        46FF3175 E33C5B4F 528BD187 1895B9B9 C01762EB 96CE6E8C
        B20B8CA7 D476D85D 35D7893C 98D5F24D 7E63CBA2 A9608156


deU is
                                                        006EF9F6
        34D00E22 A3876CBA 3732D0C9 5B3DD356 855E319B 299DFF89
        D5D6FDC4 23C76085 CC5FFB50 D2F8DE27 37B56616 9C5A63B4
```

QeU_x is

00BDA188
5B7E54B3 66D5BEC1 D652ECA6 1A395378 916541C7 935B09DB
557BC6EE 5E25FD9B BD77F039 D95ED6E9 4248FB03 B5655B44

QeU_y is

01A7E08C
BA0374A2 C0AEFAFC 41608CF1 7E718888 DCE2132E 191F4565
15EFC4B7 8C22E6B8 926C30F0 B513107B B88ABC84 FB15E337

deV is

0027B021
03628C64 7D62DD5C 457FDC78 D94CD338 66AE1C7C 509B7FDB
F04757C5 BCB1FBFB 4A55396C 368FCE29 28B9FC65 E27ACB9D

QeV_x is

01608259
EA87B351 92512DE2 094B7BB2 9BFC9591 890D922F B0EE9B15
3C9A7294 0D9D9F99 C5D90E6A 2DABD387 9DF60C7F DE9E1A82

QeV_y is

01D57627
9DA387FD 747F9D44 E7FC2701 0BB65E32 F7113315 35DBD652
031AF6BD 97EABF07 62DDC5EF 9446CDDB 2AFBA7BA 845ED2B3

---

no Key Confirmation
Zs is

01EC9EB6
3C2DD1AA 01A5795D 16031F16 5890B473 ED9BB1A8 3214E301
0A36415B 520D11F6 1FDDE602 C0A8E8B7 C7551E61 49757F66

Ze is

008B2211
0D9143CD AA3AF69F 181BF6E0 359A7093 0AE8EF77 68C2DD78
1FE6000B A089932C F5DE118F 62050E83 6D92A090 4FBA2AC2

Z is
                                                  008B2211 0D9143CD
        AA3AF69F 181BF6E0 359A7093 0AE8EF77 68C2DD78 1FE6000B
        A089932C F5DE118F 62050E83 6D92A090 4FBA2AC2 01EC9EB6
        3C2DD1AA 01A5795D 16031F16 5890B473 ED9BB1A8 3214E301
        0A36415B 520D11F6 1FDDE602 C0A8E8B7 C7551E61 49757F66

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
        1A1DBBCF 49AF6E9B 6468A478 82D78F41 4C95D516 15B996DE
        D62D6101 6D0B6512 CB94B947 90896F3A 9D0D8545 D4F35D06
        002C6A4C E2697F1B A89DE438 8DA4C9F5 1423D82A C6C733C8
        B5BFA94F 68B932F9 455EC41A 884364E1 1BA3F2A3 E1E917F9

KeyData is
        1A1DBBCF 49AF6E9B 6468A478 82D78F41 4C95D516 15B996DE
        D62D6101 6D0B6512 CB94B947 90896F3A 9D0D8545 D4F35D06
        002C6A4C E2697F1B A89DE438 8DA4C9F5 1423D82A C6C733C8
        B5BFA94F 68B932F9 455EC41A 884364E1 1BA3F2A3 E1E917F9

Scheme Initiator, Key Confirmation Provider: U to V
Zs is
                                                      01EC9EB6
        3C2DD1AA 01A5795D 16031F16 5890B473 ED9BB1A8 3214E301
        0A36415B 520D11F6 1FDDE602 C0A8E8B7 C7551E61 49757F66

Ze is
                                                      008B2211
        0D9143CD AA3AF69F 181BF6E0 359A7093 0AE8EF77 68C2DD78
        1FE6000B A089932C F5DE118F 62050E83 6D92A090 4FBA2AC2

Z is
                                                  008B2211 0D9143CD
        AA3AF69F 181BF6E0 359A7093 0AE8EF77 68C2DD78 1FE6000B
        A089932C F5DE118F 62050E83 6D92A090 4FBA2AC2 01EC9EB6

```
        3C2DD1AA 01A5795D 16031F16 5890B473 ED9BB1A8 3214E301
        0A36415B 520D11F6 1FDDE602 C0A8E8B7 C7551E61 49757F66


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        1A1DBBCF 49AF6E9B 6468A478 82D78F41 4C95D516 15B996DE
        D62D6101 6D0B6512 CB94B947 90896F3A 9D0D8545 D4F35D06
        002C6A4C E2697F1B A89DE438 8DA4C9F5 1423D82A C6C733C8
        B5BFA94F 68B932F9 455EC41A 884364E1 1BA3F2A3 E1E917F9
        F7C9487B 2A42C21B B7DCA8A9 E52A45B3 3F88F10D 075A74CC


MacData is
                                            4B435F31 5F55414C
        49434542 4F424259 00BDA188 5B7E54B3 66D5BEC1 D652ECA6
        1A395378 916541C7 935B09DB 557BC6EE 5E25FD9B BD77F039
        D95ED6E9 4248FB03 B5655B44 01A7E08C BA0374A2 C0AEFAFC
        41608CF1 7E718888 DCE2132E 191F4565 15EFC4B7 8C22E6B8
        926C30F0 B513107B B88ABC84 FB15E337 01608259 EA87B351
        92512DE2 094B7BB2 9BFC9591 890D922F B0EE9B15 3C9A7294
        0D9D9F99 C5D90E6A 2DABD387 9DF60C7F DE9E1A82 01D57627
        9DA387FD 747F9D44 E7FC2701 0BB65E32 F7113315 35DBD652
        031AF6BD 97EABF07 62DDC5EF 9446CDDB 2AFBA7BA 845ED2B3


MacKey is
        1A1DBBCF 49AF6E9B 6468A478 82D78F41 4C95D516 15B996DE


Mtag is
        1DEA50E2 ED143B5C 58E918B1 7F31C963 8CD07EDD 87A9E1C5
        342906A3 A550A6EB 70644FAB 4F1F2C25 ADA53131 73BF4428


KeyData is
        D62D6101 6D0B6512 CB94B947 90896F3A 9D0D8545 D4F35D06
        002C6A4C E2697F1B A89DE438 8DA4C9F5 1423D82A C6C733C8
        B5BFA94F 68B932F9 455EC41A 884364E1 1BA3F2A3 E1E917F9
        F7C9487B 2A42C21B B7DCA8A9 E52A45B3 3F88F10D 075A74CC
```

```
------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Zs is
                                                        01EC9EB6
        3C2DD1AA 01A5795D 16031F16 5890B473 ED9BB1A8 3214E301
        0A36415B 520D11F6 1FDDE602 C0A8E8B7 C7551E61 49757F66


Ze is
                                                        008B2211
        0D9143CD AA3AF69F 181BF6E0 359A7093 0AE8EF77 68C2DD78
        1FE6000B A089932C F5DE118F 62050E83 6D92A090 4FBA2AC2


Z is
                                                008B2211 0D9143CD
        AA3AF69F 181BF6E0 359A7093 0AE8EF77 68C2DD78 1FE6000B
        A089932C F5DE118F 62050E83 6D92A090 4FBA2AC2 01EC9EB6
        3C2DD1AA 01A5795D 16031F16 5890B473 ED9BB1A8 3214E301
        0A36415B 520D11F6 1FDDE602 C0A8E8B7 C7551E61 49757F66


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        1A1DBBCF 49AF6E9B 6468A478 82D78F41 4C95D516 15B996DE
        D62D6101 6D0B6512 CB94B947 90896F3A 9D0D8545 D4F35D06
        002C6A4C E2697F1B A89DE438 8DA4C9F5 1423D82A C6C733C8
        B5BFA94F 68B932F9 455EC41A 884364E1 1BA3F2A3 E1E917F9
        F7C9487B 2A42C21B B7DCA8A9 E52A45B3 3F88F10D 075A74CC


MacData is
                                                4B435F31 5F56424F
        42425941 4C494345 01608259 EA87B351 92512DE2 094B7BB2
        9BFC9591 890D922F B0EE9B15 3C9A7294 0D9D9F99 C5D90E6A
        2DABD387 9DF60C7F DE9E1A82 01D57627 9DA387FD 747F9D44
        E7FC2701 0BB65E32 F7113315 35DBD652 031AF6BD 97EABF07
        62DDC5EF 9446CDDB 2AFBA7BA 845ED2B3 00BDA188 5B7E54B3
        66D5BEC1 D652ECA6 1A395378 916541C7 935B09DB 557BC6EE
        5E25FD9B BD77F039 D95ED6E9 4248FB03 B5655B44 01A7E08C
        BA0374A2 C0AEFAFC 41608CF1 7E718888 DCE2132E 191F4565
        15EFC4B7 8C22E6B8 926C30F0 B513107B B88ABC84 FB15E337
```

MacKey is
        1A1DBBCF 49AF6E9B 6468A478 82D78F41 4C95D516 15B996DE

Mtag is
        7A51C0FC 7E1C5503 7FA81AE6 2FEA0565 7CF56438 EBD53667
        805CB9D5 BC7A1847 6ED4649B 16F1657A 3A4F34CB 9A71FF62

KeyData is
        D62D6101 6D0B6512 CB94B947 90896F3A 9D0D8545 D4F35D06
        002C6A4C E2697F1B A89DE438 8DA4C9F5 1423D82A C6C733C8
        B5BFA94F 68B932F9 455EC41A 884364E1 1BA3F2A3 E1E917F9
        F7C9487B 2A42C21B B7DCA8A9 E52A45B3 3F88F10D 075A74CC

Scheme Initiator, Key Confirmation Bilateral
Zs is
                                                        01EC9EB6
        3C2DD1AA 01A5795D 16031F16 5890B473 ED9BB1A8 3214E301
        0A36415B 520D11F6 1FDDE602 C0A8E8B7 C7551E61 49757F66

Ze is
                                                        008B2211
        0D9143CD AA3AF69F 181BF6E0 359A7093 0AE8EF77 68C2DD78
        1FE6000B A089932C F5DE118F 62050E83 6D92A090 4FBA2AC2

Z is
                                                008B2211 0D9143CD
        AA3AF69F 181BF6E0 359A7093 0AE8EF77 68C2DD78 1FE6000B
        A089932C F5DE118F 62050E83 6D92A090 4FBA2AC2 01EC9EB6
        3C2DD1AA 01A5795D 16031F16 5890B473 ED9BB1A8 3214E301
        0A36415B 520D11F6 1FDDE602 C0A8E8B7 C7551E61 49757F66

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

```
DerivedKeyMaterial is
        1A1DBBCF 49AF6E9B 6468A478 82D78F41 4C95D516 15B996DE
        D62D6101 6D0B6512 CB94B947 90896F3A 9D0D8545 D4F35D06
        002C6A4C E2697F1B A89DE438 8DA4C9F5 1423D82A C6C733C8
        B5BFA94F 68B932F9 455EC41A 884364E1 1BA3F2A3 E1E917F9
        F7C9487B 2A42C21B B7DCA8A9 E52A45B3 3F88F10D 075A74CC


U2V
----------------
MacData is
                                            4B435F32 5F55414C
        49434542 4F424259 00BDA188 5B7E54B3 66D5BEC1 D652ECA6
        1A395378 916541C7 935B09DB 557BC6EE 5E25FD9B BD77F039
        D95ED6E9 4248FB03 B5655B44 01A7E08C BA0374A2 C0AEFAFC
        41608CF1 7E718888 DCE2132E 191F4565 15EFC4B7 8C22E6B8
        926C30F0 B513107B B88ABC84 FB15E337 01608259 EA87B351
        92512DE2 094B7BB2 9BFC9591 890D922F B0EE9B15 3C9A7294
        0D9D9F99 C5D90E6A 2DABD387 9DF60C7F DE9E1A82 01D57627
        9DA387FD 747F9D44 E7FC2701 0BB65E32 F7113315 35DBD652
        031AF6BD 97EABF07 62DDC5EF 9446CDDB 2AFBA7BA 845ED2B3


MacKey is
        1A1DBBCF 49AF6E9B 6468A478 82D78F41 4C95D516 15B996DE


Mtag is
        DE5D0613 C3ED2213 CAED5E95 BCF79F6A FB85930F B6DC02AF
        B6DA9144 0A43A95B FCB12852 BB637FEF 7768C835 6993CD75


V2U
----------------
MacData is
                                            4B435F32 5F56424F
        42425941 4C494345 01608259 EA87B351 92512DE2 094B7BB2
        9BFC9591 890D922F B0EE9B15 3C9A7294 0D9D9F99 C5D90E6A
        2DABD387 9DF60C7F DE9E1A82 01D57627 9DA387FD 747F9D44
        E7FC2701 0BB65E32 F7113315 35DBD652 031AF6BD 97EABF07
        62DDC5EF 9446CDDB 2AFBA7BA 845ED2B3 00BDA188 5B7E54B3
        66D5BEC1 D652ECA6 1A395378 916541C7 935B09DB 557BC6EE
        5E25FD9B BD77F039 D95ED6E9 4248FB03 B5655B44 01A7E08C
        BA0374A2 C0AEFAFC 41608CF1 7E718888 DCE2132E 191F4565
        15EFC4B7 8C22E6B8 926C30F0 B513107B B88ABC84 FB15E337
```

MacKey is
        1A1DBBCF 49AF6E9B 6468A478 82D78F41 4C95D516 15B996DE

Mtag is
        C53067FA F397DCF0 F7A2F7BB D09FDEBE 7599AB94 E4C06233
        1EAB8DC3 0C5E3BA5 60994564 B5703E8D 877B61C2 5DBAB72E

KeyData is
        D62D6101 6D0B6512 CB94B947 90896F3A 9D0D8545 D4F35D06
        002C6A4C E2697F1B A89DE438 8DA4C9F5 1423D82A C6C733C8
        B5BFA94F 68B932F9 455EC41A 884364E1 1BA3F2A3 E1E917F9
        F7C9487B 2A42C21B B7DCA8A9 E52A45B3 3F88F10D 075A74CC

FullMQV(K-409)
----
dsU is
                                                        0072A861
        311C6905 1FA44C65 A2153631 F19A443F 6B882C28 F4F9C762
        EF30092B 703809D7 5C0892C2 81BA205C 5D870D63 A769033D

QsU_x is
                                                        0152E7F8
        335C1766 4DA0AE5C 7362B49E 14E68453 21768152 5510421F
        A24F5F07 AB1DF096 79398A1F AABF279D 3C44F214 E96DB92A

QsU_y is
                                                        002E3FEF
        D35E52C0 10EBAAD3 C5DBEAF6 9868E630 7D0DAC71 2C7B736D
        474666F9 8B880A5B 25E3B6BA 10098EA8 8AF8FA0E 3C5F4A8D

dsV is
                                                        0047F7DF
        0EB84625 BFE69F8C 9DE845AF A5A26EDD C41B6B56 47360A53
        71398245 8EA0231A F2DA0BAE FA71EB6C 05E1B7D0 837BBFA1

QsV_x is

                                                    0107C00B
        AB1A1085 9172E54E B34DC8BE 22ECCAF9 08E65F4E B97BF481
        F86C0B15 DB869112 8CABD886 9CDDC529 B48AFF82 819A79D0

QsV_y is
                                                    01321631
        46FF3175 E33C5B4F 528BD187 1895B9B9 C01762EB 96CE6E8C
        B20B8CA7 D476D85D 35D7893C 98D5F24D 7E63CBA2 A9608156

deU is
                                                    006EF9F6
        34D00E22 A3876CBA 3732D0C9 5B3DD356 855E319B 299DFF89
        D5D6FDC4 23C76085 CC5FFB50 D2F8DE27 37B56616 9C5A63B4

QeU_x is
                                                    00BDA188
        5B7E54B3 66D5BEC1 D652ECA6 1A395378 916541C7 935B09DB
        557BC6EE 5E25FD9B BD77F039 D95ED6E9 4248FB03 B5655B44

QeU_y is
                                                    01A7E08C
        BA0374A2 C0AEFAFC 41608CF1 7E718888 DCE2132E 191F4565
        15EFC4B7 8C22E6B8 926C30F0 B513107B B88ABC84 FB15E337

deV is
                                                    0027B021
        03628C64 7D62DD5C 457FDC78 D94CD338 66AE1C7C 509B7FDB
        F04757C5 BCB1FBFB 4A55396C 368FCE29 28B9FC65 E27ACB9D

QeV_x is
                                                    01608259
        EA87B351 92512DE2 094B7BB2 9BFC9591 890D922F B0EE9B15
        3C9A7294 0D9D9F99 C5D90E6A 2DABD387 9DF60C7F DE9E1A82

QeV_y is
                                                    01D57627
        9DA387FD 747F9D44 E7FC2701 0BB65E32 F7113315 35DBD652
        031AF6BD 97EABF07 62DDC5EF 9446CDDB 2AFBA7BA 845ED2B3

```
------------------------------------------------------------
no Key Confirmation
Z is
                                                        0027593C
        D8C8A2FA BD7BB03A B886E9E0 E8FAA1CC FAC290A9 94831E79
        24961F59 2103548D A6123045 FAE16EF5 C6441B03 204A205C


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        27A233EB 4B7425E9 EE97826E FF2708E9 0F2122BB B394794E
        12C9C46E 37364CB6 7EC01A5F CEBECBA6 2AA5366E 308B5FEB
        D55F5740 11182C7C 7275E28A 0079DE26 DAD98A7F 158AFE4D
        12FBB1CF 22B2BA38 5EADA734 1FBDE353 D8F5C938 BA241ADD


KeyData is
        27A233EB 4B7425E9 EE97826E FF2708E9 0F2122BB B394794E
        12C9C46E 37364CB6 7EC01A5F CEBECBA6 2AA5366E 308B5FEB
        D55F5740 11182C7C 7275E28A 0079DE26 DAD98A7F 158AFE4D
        12FBB1CF 22B2BA38 5EADA734 1FBDE353 D8F5C938 BA241ADD




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Z is
                                                        0027593C
        D8C8A2FA BD7BB03A B886E9E0 E8FAA1CC FAC290A9 94831E79
        24961F59 2103548D A6123045 FAE16EF5 C6441B03 204A205C


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        27A233EB 4B7425E9 EE97826E FF2708E9 0F2122BB B394794E
        12C9C46E 37364CB6 7EC01A5F CEBECBA6 2AA5366E 308B5FEB
```

D55F5740 11182C7C 7275E28A 0079DE26 DAD98A7F 158AFE4D
12FBB1CF 22B2BA38 5EADA734 1FBDE353 D8F5C938 BA241ADD
761D7023 A4E1F224 A92CFFC7 86F83C19 ACD95DE9 FE005FCD

MacData is
4B435F31 5F55414C
49434542 4F424259 00BDA188 5B7E54B3 66D5BEC1 D652ECA6
1A395378 916541C7 935B09DB 557BC6EE 5E25FD9B BD77F039
D95ED6E9 4248FB03 B5655B44 01A7E08C BA0374A2 C0AEFAFC
41608CF1 7E718888 DCE2132E 191F4565 15EFC4B7 8C22E6B8
926C30F0 B513107B B88ABC84 FB15E337 01608259 EA87B351
92512DE2 094B7BB2 9BFC9591 890D922F B0EE9B15 3C9A7294
0D9D9F99 C5D90E6A 2DABD387 9DF60C7F DE9E1A82 01D57627
9DA387FD 747F9D44 E7FC2701 0BB65E32 F7113315 35DBD652
031AF6BD 97EABF07 62DDC5EF 9446CDDB 2AFBA7BA 845ED2B3

MacKey is
27A233EB 4B7425E9 EE97826E FF2708E9 0F2122BB B394794E

Mtag is
E3E2C9F6 341FA65B 596C6373 51FD7EA0 DD91BE56 C7D47A72
02A4FB10 D3B518A5 F76253E2 E58E0C69 B7C47201 2849FF72

KeyData is
12C9C46E 37364CB6 7EC01A5F CEBECBA6 2AA5366E 308B5FEB
D55F5740 11182C7C 7275E28A 0079DE26 DAD98A7F 158AFE4D
12FBB1CF 22B2BA38 5EADA734 1FBDE353 D8F5C938 BA241ADD
761D7023 A4E1F224 A92CFFC7 86F83C19 ACD95DE9 FE005FCD

Scheme Responder, Key Confirmation Provider: V to U
Z is
0027593C
D8C8A2FA BD7BB03A B886E9E0 E8FAA1CC FAC290A9 94831E79
24961F59 2103548D A6123045 FAE16EF5 C6441B03 204A205C

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

```
DerivedKeyMaterial is
        27A233EB 4B7425E9 EE97826E FF2708E9 0F2122BB B394794E
        12C9C46E 37364CB6 7EC01A5F CEBECBA6 2AA5366E 308B5FEB
        D55F5740 11182C7C 7275E28A 0079DE26 DAD98A7F 158AFE4D
        12FBB1CF 22B2BA38 5EADA734 1FBDE353 D8F5C938 BA241ADD
        761D7023 A4E1F224 A92CFFC7 86F83C19 ACD95DE9 FE005FCD


MacData is
                                            4B435F31 5F56424F
        42425941 4C494345 01608259 EA87B351 92512DE2 094B7BB2
        9BFC9591 890D922F B0EE9B15 3C9A7294 0D9D9F99 C5D90E6A
        2DABD387 9DF60C7F DE9E1A82 01D57627 9DA387FD 747F9D44
        E7FC2701 0BB65E32 F7113315 35DBD652 031AF6BD 97EABF07
        62DDC5EF 9446CDDB 2AFBA7BA 845ED2B3 00BDA188 5B7E54B3
        66D5BEC1 D652ECA6 1A395378 916541C7 935B09DB 557BC6EE
        5E25FD9B BD77F039 D95ED6E9 4248FB03 B5655B44 01A7E08C
        BA0374A2 C0AEFAFC 41608CF1 7E718888 DCE2132E 191F4565
        15EFC4B7 8C22E6B8 926C30F0 B513107B B88ABC84 FB15E337


MacKey is
        27A233EB 4B7425E9 EE97826E FF2708E9 0F2122BB B394794E


Mtag is
        3E4F9F2A 520A48DD A473155F 01C3CD9B B545B247 39FDED40
        6E714D6D F2D2BC94 3CED64AB 44DB23F4 3B6A8226 46F6B078


KeyData is
        12C9C46E 37364CB6 7EC01A5F CEBECBA6 2AA5366E 308B5FEB
        D55F5740 11182C7C 7275E28A 0079DE26 DAD98A7F 158AFE4D
        12FBB1CF 22B2BA38 5EADA734 1FBDE353 D8F5C938 BA241ADD
        761D7023 A4E1F224 A92CFFC7 86F83C19 ACD95DE9 FE005FCD




-------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
Z is
                                                    0027593C
```

```
        D8C8A2FA BD7BB03A B886E9E0 E8FAA1CC FAC290A9 94831E79
        24961F59 2103548D A6123045 FAE16EF5 C6441B03 204A205C


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        27A233EB 4B7425E9 EE97826E FF2708E9 0F2122BB B394794E
        12C9C46E 37364CB6 7EC01A5F CEBECBA6 2AA5366E 308B5FEB
        D55F5740 11182C7C 7275E28A 0079DE26 DAD98A7F 158AFE4D
        12FBB1CF 22B2BA38 5EADA734 1FBDE353 D8F5C938 BA241ADD
        761D7023 A4E1F224 A92CFFC7 86F83C19 ACD95DE9 FE005FCD


U2V
----------------
MacData is
                                            4B435F32 5F55414C
        49434542 4F424259 00BDA188 5B7E54B3 66D5BEC1 D652ECA6
        1A395378 916541C7 935B09DB 557BC6EE 5E25FD9B BD77F039
        D95ED6E9 4248FB03 B5655B44 01A7E08C BA0374A2 C0AEFAFC
        41608CF1 7E718888 DCE2132E 191F4565 15EFC4B7 8C22E6B8
        926C30F0 B513107B B88ABC84 FB15E337 01608259 EA87B351
        92512DE2 094B7BB2 9BFC9591 890D922F B0EE9B15 3C9A7294
        0D9D9F99 C5D90E6A 2DABD387 9DF60C7F DE9E1A82 01D57627
        9DA387FD 747F9D44 E7FC2701 0BB65E32 F7113315 35DBD652
        031AF6BD 97EABF07 62DDC5EF 9446CDDB 2AFBA7BA 845ED2B3


MacKey is
        27A233EB 4B7425E9 EE97826E FF2708E9 0F2122BB B394794E


Mtag is
        EC1704E5 82BD6478 62862251 973E0C30 11475451 9E4DDAC4
        1640ED30 054286FD BE7FCAD5 EA5E1909 7EB715FD D19172F6


V2U
----------------
MacData is
                                            4B435F32 5F56424F
        42425941 4C494345 01608259 EA87B351 92512DE2 094B7BB2
        9BFC9591 890D922F B0EE9B15 3C9A7294 0D9D9F99 C5D90E6A
```

```
        2DABD387 9DF60C7F DE9E1A82 01D57627 9DA387FD 747F9D44
        E7FC2701 0BB65E32 F7113315 35DBD652 031AF6BD 97EABF07
        62DDC5EF 9446CDDB 2AFBA7BA 845ED2B3 00BDA188 5B7E54B3
        66D5BEC1 D652ECA6 1A395378 916541C7 935B09DB 557BC6EE
        5E25FD9B BD77F039 D95ED6E9 4248FB03 B5655B44 01A7E08C
        BA0374A2 C0AEFAFC 41608CF1 7E718888 DCE2132E 191F4565
        15EFC4B7 8C22E6B8 926C30F0 B513107B B88ABC84 FB15E337


MacKey is
        27A233EB 4B7425E9 EE97826E FF2708E9 0F2122BB B394794E


Mtag is
        004D4200 6CE16CA8 980C5D95 1BA64951 92914C2B D4D9EBDC
        521D939A 5DE9175D E26FCA00 A9A2427A 847C86E0 F69BCCF3


KeyData is
        12C9C46E 37364CB6 7EC01A5F CEBECBA6 2AA5366E 308B5FEB
        D55F5740 11182C7C 7275E28A 0079DE26 DAD98A7F 158AFE4D
        12FBB1CF 22B2BA38 5EADA734 1FBDE353 D8F5C938 BA241ADD
        761D7023 A4E1F224 A92CFFC7 86F83C19 ACD95DE9 FE005FCD




EphemeralUnifiedCDH(K-409)
------------------------------------------------------------
deU is
                                                        006EF9F6
        34D00E22 A3876CBA 3732D0C9 5B3DD356 855E319B 299DFF89
        D5D6FDC4 23C76085 CC5FFB50 D2F8DE27 37B56616 9C5A63B4


QeU_x is
                                                        00BDA188
        5B7E54B3 66D5BEC1 D652ECA6 1A395378 916541C7 935B09DB
        557BC6EE 5E25FD9B BD77F039 D95ED6E9 4248FB03 B5655B44


QeU_y is
                                                        01A7E08C
        BA0374A2 C0AEFAFC 41608CF1 7E718888 DCE2132E 191F4565
        15EFC4B7 8C22E6B8 926C30F0 B513107B B88ABC84 FB15E337
```

```
deV is
                                                        0027B021
        03628C64 7D62DD5C 457FDC78 D94CD338 66AE1C7C 509B7FDB
        F04757C5 BCB1FBFB 4A55396C 368FCE29 28B9FC65 E27ACB9D


QeV_x is
                                                        01608259
        EA87B351 92512DE2 094B7BB2 9BFC9591 890D922F B0EE9B15
        3C9A7294 0D9D9F99 C5D90E6A 2DABD387 9DF60C7F DE9E1A82


QeV_y is
                                                        01D57627
        9DA387FD 747F9D44 E7FC2701 0BB65E32 F7113315 35DBD652
        031AF6BD 97EABF07 62DDC5EF 9446CDDB 2AFBA7BA 845ED2B3




------------------------------------------------------------
no Key Confirmation
Z is
                                                        008B2211
        0D9143CD AA3AF69F 181BF6E0 359A7093 0AE8EF77 68C2DD78
        1FE6000B A089932C F5DE118F 62050E83 6D92A090 4FBA2AC2


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        20C9C72A B17FE14F 24B3FF21 3480D4CC A9FD616C ECDDC5E3
        C28EF1AD 0CB89544 72478709 93367D10 564A84CF 949E9FEE
        CF4A6D52 B6764976 2ECA35E2 73DF819A 7119013A 882D28B6
        34D1E58A BF11B2AF E502C8AE 8B0F94C5 A62F192F BE80136B


KeyData is
        20C9C72A B17FE14F 24B3FF21 3480D4CC A9FD616C ECDDC5E3
        C28EF1AD 0CB89544 72478709 93367D10 564A84CF 949E9FEE
        CF4A6D52 B6764976 2ECA35E2 73DF819A 7119013A 882D28B6
        34D1E58A BF11B2AF E502C8AE 8B0F94C5 A62F192F BE80136B
```

OnePassUnifiedCDH(K-409)
---
dsU is
0072A861
311C6905 1FA44C65 A2153631 F19A443F 6B882C28 F4F9C762
EF30092B 703809D7 5C0892C2 81BA205C 5D870D63 A769033D

QsU_x is
0152E7F8
335C1766 4DA0AE5C 7362B49E 14E68453 21768152 5510421F
A24F5F07 AB1DF096 79398A1F AABF279D 3C44F214 E96DB92A

QsU_y is
002E3FEF
D35E52C0 10EBAAD3 C5DBEAF6 9868E630 7D0DAC71 2C7B736D
474666F9 8B880A5B 25E3B6BA 10098EA8 8AF8FA0E 3C5F4A8D

dsV is
0047F7DF
0EB84625 BFE69F8C 9DE845AF A5A26EDD C41B6B56 47360A53
71398245 8EA0231A F2DA0BAE FA71EB6C 05E1B7D0 837BBFA1

QsV_x is
0107C00B
AB1A1085 9172E54E B34DC8BE 22ECCAF9 08E65F4E B97BF481
F86C0B15 DB869112 8CABD886 9CDDC529 B48AFF82 819A79D0

QsV_y is
01321631
46FF3175 E33C5B4F 528BD187 1895B9B9 C01762EB 96CE6E8C
B20B8CA7 D476D85D 35D7893C 98D5F24D 7E63CBA2 A9608156

deU is
006EF9F6
34D00E22 A3876CBA 3732D0C9 5B3DD356 855E319B 299DFF89
D5D6FDC4 23C76085 CC5FFB50 D2F8DE27 37B56616 9C5A63B4

QeU_x is
                                                        00BDA188
        5B7E54B3 66D5BEC1 D652ECA6 1A395378 916541C7 935B09DB
        557BC6EE 5E25FD9B BD77F039 D95ED6E9 4248FB03 B5655B44

QeU_y is
                                                        01A7E08C
        BA0374A2 C0AEFAFC 41608CF1 7E718888 DCE2132E 191F4565
        15EFC4B7 8C22E6B8 926C30F0 B513107B B88ABC84 FB15E337

---

no Key Confirmation
Zs is
                                                        01EC9EB6
        3C2DD1AA 01A5795D 16031F16 5890B473 ED9BB1A8 3214E301
        0A36415B 520D11F6 1FDDE602 C0A8E8B7 C7551E61 49757F66

Ze is
                                                        000AD809
        4E7EA41A 4EC724DC B2621062 C0BEAE30 71A83480 C7357E40
        91468F86 7B5EDE0E 0D2ECB8A ED3A8463 C91E1F82 A855D0A2

Z is
                                                000AD809 4E7EA41A
        4EC724DC B2621062 C0BEAE30 71A83480 C7357E40 91468F86
        7B5EDE0E 0D2ECB8A ED3A8463 C91E1F82 A855D0A2 01EC9EB6
        3C2DD1AA 01A5795D 16031F16 5890B473 ED9BB1A8 3214E301
        0A36415B 520D11F6 1FDDE602 C0A8E8B7 C7551E61 49757F66

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
        E65680DF 3EC346F3 0324D8B7 C3175828 CEA32637 91A1B8A1
        53D2E2DA 23D64217 83970E3F B0736F7C 549C9D0A 5F7B6E52
        1C373C0A 00FDE027 83981FAA 5E78ACE0 52D379CD F3617250
        48538AFF 2E191B92 C6C293F9 B069104C 5CB6D493 6E59A2BB

KeyData is
        E65680DF 3EC346F3 0324D8B7 C3175828 CEA32637 91A1B8A1
        53D2E2DA 23D64217 83970E3F B0736F7C 549C9D0A 5F7B6E52
        1C373C0A 00FDE027 83981FAA 5E78ACE0 52D379CD F3617250
        48538AFF 2E191B92 C6C293F9 B069104C 5CB6D493 6E59A2BB

Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                                                    0010F0B2
        F19A11B5 B520AC95 8B15B47F 40A0D1BA 2D7B4E22 7EBDB816
        24732755 E6E1FBD4 05EA97CD 22E40D68 E96FF680 07412421

Zs is
                                                    01EC9EB6
        3C2DD1AA 01A5795D 16031F16 5890B473 ED9BB1A8 3214E301
        0A36415B 520D11F6 1FDDE602 C0A8E8B7 C7551E61 49757F66

Ze is
                                                    000AD809
        4E7EA41A 4EC724DC B2621062 C0BEAE30 71A83480 C7357E40
        91468F86 7B5EDE0E 0D2ECB8A ED3A8463 C91E1F82 A855D0A2

Z is
                                            000AD809 4E7EA41A
        4EC724DC B2621062 C0BEAE30 71A83480 C7357E40 91468F86
        7B5EDE0E 0D2ECB8A ED3A8463 C91E1F82 A855D0A2 01EC9EB6
        3C2DD1AA 01A5795D 16031F16 5890B473 ED9BB1A8 3214E301
        0A36415B 520D11F6 1FDDE602 C0A8E8B7 C7551E61 49757F66

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
        E65680DF 3EC346F3 0324D8B7 C3175828 CEA32637 91A1B8A1
        53D2E2DA 23D64217 83970E3F B0736F7C 549C9D0A 5F7B6E52

```
        1C373C0A 00FDE027 83981FAA 5E78ACE0 52D379CD F3617250
        48538AFF 2E191B92 C6C293F9 B069104C 5CB6D493 6E59A2BB
        8C0F37EC 31DE0231 486C667B 56E02B65 C23DA7FB DD4ED6BF


MacData is
                                                    4B435F31
        5F55414C 49434542 4F424259 00BDA188 5B7E54B3 66D5BEC1
        D652ECA6 1A395378 916541C7 935B09DB 557BC6EE 5E25FD9B
        BD77F039 D95ED6E9 4248FB03 B5655B44 01A7E08C BA0374A2
        C0AEFAFC 41608CF1 7E718888 DCE2132E 191F4565 15EFC4B7
        8C22E6B8 926C30F0 B513107B B88ABC84 FB15E337 0010F0B2
        F19A11B5 B520AC95 8B15B47F 40A0D1BA 2D7B4E22 7EBDB816
        24732755 E6E1FBD4 05EA97CD 22E40D68 E96FF680 07412421


MacKey is
        E65680DF 3EC346F3 0324D8B7 C3175828 CEA32637 91A1B8A1


Mtag is
        53EABF8D 6D31D311 FDBD59DC F6D2AD60 79CB0197 CE025591
        B1ED80A1 3EFA93DD 356AEC6D 2D6DB45E A821E4F1 85DD98F8


KeyData is
        53D2E2DA 23D64217 83970E3F B0736F7C 549C9D0A 5F7B6E52
        1C373C0A 00FDE027 83981FAA 5E78ACE0 52D379CD F3617250
        48538AFF 2E191B92 C6C293F9 B069104C 5CB6D493 6E59A2BB
        8C0F37EC 31DE0231 486C667B 56E02B65 C23DA7FB DD4ED6BF




-------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
                                                    0010F0B2
        F19A11B5 B520AC95 8B15B47F 40A0D1BA 2D7B4E22 7EBDB816
        24732755 E6E1FBD4 05EA97CD 22E40D68 E96FF680 07412421


Zs is
                                                    01EC9EB6
        3C2DD1AA 01A5795D 16031F16 5890B473 ED9BB1A8 3214E301
        0A36415B 520D11F6 1FDDE602 C0A8E8B7 C7551E61 49757F66
```

Ze is
                                                    000AD809
        4E7EA41A 4EC724DC B2621062 C0BEAE30 71A83480 C7357E40
        91468F86 7B5EDE0E 0D2ECB8A ED3A8463 C91E1F82 A855D0A2

Z is
                                            000AD809 4E7EA41A
        4EC724DC B2621062 C0BEAE30 71A83480 C7357E40 91468F86
        7B5EDE0E 0D2ECB8A ED3A8463 C91E1F82 A855D0A2 01EC9EB6
        3C2DD1AA 01A5795D 16031F16 5890B473 ED9BB1A8 3214E301
        0A36415B 520D11F6 1FDDE602 C0A8E8B7 C7551E61 49757F66

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
        E65680DF 3EC346F3 0324D8B7 C3175828 CEA32637 91A1B8A1
        53D2E2DA 23D64217 83970E3F B0736F7C 549C9D0A 5F7B6E52
        1C373C0A 00FDE027 83981FAA 5E78ACE0 52D379CD F3617250
        48538AFF 2E191B92 C6C293F9 B069104C 5CB6D493 6E59A2BB
        8C0F37EC 31DE0231 486C667B 56E02B65 C23DA7FB DD4ED6BF

MacData is
        4B435F31 5F56424F 42425941 4C494345 00BDA188 5B7E54B3
        66D5BEC1 D652ECA6 1A395378 916541C7 935B09DB 557BC6EE
        5E25FD9B BD77F039 D95ED6E9 4248FB03 B5655B44 01A7E08C
        BA0374A2 C0AEFAFC 41608CF1 7E718888 DCE2132E 191F4565
        15EFC4B7 8C22E6B8 926C30F0 B513107B B88ABC84 FB15E337

MacKey is
        E65680DF 3EC346F3 0324D8B7 C3175828 CEA32637 91A1B8A1

Mtag is
        8F1FB6F2 933DFDFE 02AD6A81 F0EAD7FE 14E4BF89 DDF76ED6
        BF560EF7 9AEAE986 A22A4B79 38B3E1C2 C2B4214E E08536D3

KeyData is

53D2E2DA 23D64217 83970E3F B0736F7C 549C9D0A 5F7B6E52
1C373C0A 00FDE027 83981FAA 5E78ACE0 52D379CD F3617250
48538AFF 2E191B92 C6C293F9 B069104C 5CB6D493 6E59A2BB
8C0F37EC 31DE0231 486C667B 56E02B65 C23DA7FB DD4ED6BF

Scheme Initiator, Key Confirmation Bilateral
NonceV is
0010F0B2
F19A11B5 B520AC95 8B15B47F 40A0D1BA 2D7B4E22 7EBDB816
24732755 E6E1FBD4 05EA97CD 22E40D68 E96FF680 07412421

Zs is
01EC9EB6
3C2DD1AA 01A5795D 16031F16 5890B473 ED9BB1A8 3214E301
0A36415B 520D11F6 1FDDE602 C0A8E8B7 C7551E61 49757F66

Ze is
000AD809
4E7EA41A 4EC724DC B2621062 C0BEAE30 71A83480 C7357E40
91468F86 7B5EDE0E 0D2ECB8A ED3A8463 C91E1F82 A855D0A2

Z is
000AD809 4E7EA41A
4EC724DC B2621062 C0BEAE30 71A83480 C7357E40 91468F86
7B5EDE0E 0D2ECB8A ED3A8463 C91E1F82 A855D0A2 01EC9EB6
3C2DD1AA 01A5795D 16031F16 5890B473 ED9BB1A8 3214E301
0A36415B 520D11F6 1FDDE602 C0A8E8B7 C7551E61 49757F66

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
E65680DF 3EC346F3 0324D8B7 C3175828 CEA32637 91A1B8A1
53D2E2DA 23D64217 83970E3F B0736F7C 549C9D0A 5F7B6E52
1C373C0A 00FDE027 83981FAA 5E78ACE0 52D379CD F3617250
48538AFF 2E191B92 C6C293F9 B069104C 5CB6D493 6E59A2BB
8C0F37EC 31DE0231 486C667B 56E02B65 C23DA7FB DD4ED6BF

U2V

MacData is
                                                        4B435F32
        5F55414C 49434542 4F424259 00BDA188 5B7E54B3 66D5BEC1
        D652ECA6 1A395378 916541C7 935B09DB 557BC6EE 5E25FD9B
        BD77F039 D95ED6E9 4248FB03 B5655B44 01A7E08C BA0374A2
        C0AEFAFC 41608CF1 7E718888 DCE2132E 191F4565 15EFC4B7
        8C22E6B8 926C30F0 B513107B B88ABC84 FB15E337 0010F0B2
        F19A11B5 B520AC95 8B15B47F 40A0D1BA 2D7B4E22 7EBDB816
        24732755 E6E1FBD4 05EA97CD 22E40D68 E96FF680 07412421

MacKey is
        E65680DF 3EC346F3 0324D8B7 C3175828 CEA32637 91A1B8A1

Mtag is
        DAEA72A5 EF479CA0 2FF5B42A CDDB03E8 67D7C4B0 793F7D65
        9405FB32 7573FA24 FB97E3EC 71BA657B 0B3146A9 974C576D

V2U

MacData is
                                                        4B435F32
        5F56424F 42425941 4C494345 0010F0B2 F19A11B5 B520AC95
        8B15B47F 40A0D1BA 2D7B4E22 7EBDB816 24732755 E6E1FBD4
        05EA97CD 22E40D68 E96FF680 07412421 00BDA188 5B7E54B3
        66D5BEC1 D652ECA6 1A395378 916541C7 935B09DB 557BC6EE
        5E25FD9B BD77F039 D95ED6E9 4248FB03 B5655B44 01A7E08C
        BA0374A2 C0AEFAFC 41608CF1 7E718888 DCE2132E 191F4565
        15EFC4B7 8C22E6B8 926C30F0 B513107B B88ABC84 FB15E337

MacKey is
        E65680DF 3EC346F3 0324D8B7 C3175828 CEA32637 91A1B8A1

Mtag is
        626B634B F5F814F4 2BE3BA47 0A94A4E8 31C4F614 B748D585
        0C712BCE 546F5954 A9A36592 86E951CE 60BEE3C2 C2AE5CD0

KeyData is
	53D2E2DA 23D64217 83970E3F B0736F7C 549C9D0A 5F7B6E52
	1C373C0A 00FDE027 83981FAA 5E78ACE0 52D379CD F3617250
	48538AFF 2E191B92 C6C293F9 B069104C 5CB6D493 6E59A2BB
	8C0F37EC 31DE0231 486C667B 56E02B65 C23DA7FB DD4ED6BF

OnePassMQV(K-409)
---
dsU is
	0072A861
	311C6905 1FA44C65 A2153631 F19A443F 6B882C28 F4F9C762
	EF30092B 703809D7 5C0892C2 81BA205C 5D870D63 A769033D

QsU_x is
	0152E7F8
	335C1766 4DA0AE5C 7362B49E 14E68453 21768152 5510421F
	A24F5F07 AB1DF096 79398A1F AABF279D 3C44F214 E96DB92A

QsU_y is
	002E3FEF
	D35E52C0 10EBAAD3 C5DBEAF6 9868E630 7D0DAC71 2C7B736D
	474666F9 8B880A5B 25E3B6BA 10098EA8 8AF8FA0E 3C5F4A8D

dsV is
	0047F7DF
	0EB84625 BFE69F8C 9DE845AF A5A26EDD C41B6B56 47360A53
	71398245 8EA0231A F2DA0BAE FA71EB6C 05E1B7D0 837BBFA1

QsV_x is
	0107C00B
	AB1A1085 9172E54E B34DC8BE 22ECCAF9 08E65F4E B97BF481
	F86C0B15 DB869112 8CABD886 9CDDC529 B48AFF82 819A79D0

QsV_y is
	01321631
	46FF3175 E33C5B4F 528BD187 1895B9B9 C01762EB 96CE6E8C
	B20B8CA7 D476D85D 35D7893C 98D5F24D 7E63CBA2 A9608156

```
deU is
                                                        006EF9F6
        34D00E22 A3876CBA 3732D0C9 5B3DD356 855E319B 299DFF89
        D5D6FDC4 23C76085 CC5FFB50 D2F8DE27 37B56616 9C5A63B4


QeU_x is
                                                        00BDA188
        5B7E54B3 66D5BEC1 D652ECA6 1A395378 916541C7 935B09DB
        557BC6EE 5E25FD9B BD77F039 D95ED6E9 4248FB03 B5655B44


QeU_y is
                                                        01A7E08C
        BA0374A2 C0AEFAFC 41608CF1 7E718888 DCE2132E 191F4565
        15EFC4B7 8C22E6B8 926C30F0 B513107B B88ABC84 FB15E337




------------------------------------------------------------
no Key Confirmation
Z is
                                                        004355F7
        D66FE5C6 333D6C57 B6BD562D 25EA51F5 9D5EAFCC E6A17F78
        0A52FEC8 726E11F0 075AAD5E 33BA4106 ACEAD43D 8F294F18


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        8909314B 9FA1C205 7F624010 8F62526B 6B3268FE 2C3F0E74
        53D16A7A 9B0DA0B3 F27B46B3 58E0D979 9DBE02FF 28E1F588
        29B4DCD4 7996CA03 2805271A 2FBFF363 E9C83263 D73C0B71
        13004EA6 5FE549D7 56B6F624 6FFC4FB0 39CAAD10 E4FBD96E


KeyData is
        8909314B 9FA1C205 7F624010 8F62526B 6B3268FE 2C3F0E74
        53D16A7A 9B0DA0B3 F27B46B3 58E0D979 9DBE02FF 28E1F588
        29B4DCD4 7996CA03 2805271A 2FBFF363 E9C83263 D73C0B71
        13004EA6 5FE549D7 56B6F624 6FFC4FB0 39CAAD10 E4FBD96E
```

Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                                                    0010F0B2
        F19A11B5 B520AC95 8B15B47F 40A0D1BA 2D7B4E22 7EBDB816
        24732755 E6E1FBD4 05EA97CD 22E40D68 E96FF680 07412421

Z is
                                                    004355F7
        D66FE5C6 333D6C57 B6BD562D 25EA51F5 9D5EAFCC E6A17F78
        0A52FEC8 726E11F0 075AAD5E 33BA4106 ACEAD43D 8F294F18

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
        8909314B 9FA1C205 7F624010 8F62526B 6B3268FE 2C3F0E74
        53D16A7A 9B0DA0B3 F27B46B3 58E0D979 9DBE02FF 28E1F588
        29B4DCD4 7996CA03 2805271A 2FBFF363 E9C83263 D73C0B71
        13004EA6 5FE549D7 56B6F624 6FFC4FB0 39CAAD10 E4FBD96E
        F2E4D022 F5A9ED57 932707B6 7F5C182D E9008AB5 EF9CEFE5

MacData is
                                                    4B435F31
        5F55414C 49434542 4F424259 00BDA188 5B7E54B3 66D5BEC1
        D652ECA6 1A395378 916541C7 935B09DB 557BC6EE 5E25FD9B
        BD77F039 D95ED6E9 4248FB03 B5655B44 01A7E08C BA0374A2
        C0AEFAFC 41608CF1 7E718888 DCE2132E 191F4565 15EFC4B7
        8C22E6B8 926C30F0 B513107B B88ABC84 FB15E337 0010F0B2
        F19A11B5 B520AC95 8B15B47F 40A0D1BA 2D7B4E22 7EBDB816
        24732755 E6E1FBD4 05EA97CD 22E40D68 E96FF680 07412421

MacKey is
        8909314B 9FA1C205 7F624010 8F62526B 6B3268FE 2C3F0E74

Mtag is
        1D0E7D4D E9095C3F 9F3202FC 411690AF FDA91710 419F96FC

```
        1694518A 82A5BA8D 552FBAD2 622B4F47 EC4C9AE9 037E2CB8


KeyData is
        53D16A7A 9B0DA0B3 F27B46B3 58E0D979 9DBE02FF 28E1F588
        29B4DCD4 7996CA03 2805271A 2FBFF363 E9C83263 D73C0B71
        13004EA6 5FE549D7 56B6F624 6FFC4FB0 39CAAD10 E4FBD96E
        F2E4D022 F5A9ED57 932707B6 7F5C182D E9008AB5 EF9CEFE5




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
                                                    0010F0B2
        F19A11B5 B520AC95 8B15B47F 40A0D1BA 2D7B4E22 7EBDB816
        24732755 E6E1FBD4 05EA97CD 22E40D68 E96FF680 07412421


Z is
                                                    004355F7
        D66FE5C6 333D6C57 B6BD562D 25EA51F5 9D5EAFCC E6A17F78
        0A52FEC8 726E11F0 075AAD5E 33BA4106 ACEAD43D 8F294F18


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        8909314B 9FA1C205 7F624010 8F62526B 6B3268FE 2C3F0E74
        53D16A7A 9B0DA0B3 F27B46B3 58E0D979 9DBE02FF 28E1F588
        29B4DCD4 7996CA03 2805271A 2FBFF363 E9C83263 D73C0B71
        13004EA6 5FE549D7 56B6F624 6FFC4FB0 39CAAD10 E4FBD96E
        F2E4D022 F5A9ED57 932707B6 7F5C182D E9008AB5 EF9CEFE5


MacData is
        4B435F31 5F56424F 42425941 4C494345 00BDA188 5B7E54B3
        66D5BEC1 D652ECA6 1A395378 916541C7 935B09DB 557BC6EE
        5E25FD9B BD77F039 D95ED6E9 4248FB03 B5655B44 01A7E08C
        BA0374A2 C0AEFAFC 41608CF1 7E718888 DCE2132E 191F4565
        15EFC4B7 8C22E6B8 926C30F0 B513107B B88ABC84 FB15E337
```

MacKey is
        8909314B 9FA1C205 7F624010 8F62526B 6B3268FE 2C3F0E74

Mtag is
        0559F877 B6A18A96 09BA779C 76070295 D653B1AB DDCD96E5
        AFB3594D 03C9E3A3 9A3E152F 9377A647 18F01125 9FA6CA0B

KeyData is
        53D16A7A 9B0DA0B3 F27B46B3 58E0D979 9DBE02FF 28E1F588
        29B4DCD4 7996CA03 2805271A 2FBFF363 E9C83263 D73C0B71
        13004EA6 5FE549D7 56B6F624 6FFC4FB0 39CAAD10 E4FBD96E
        F2E4D022 F5A9ED57 932707B6 7F5C182D E9008AB5 EF9CEFE5

Scheme Initiator, Key Confirmation Bilateral
NonceV is
                                                    0010F0B2
        F19A11B5 B520AC95 8B15B47F 40A0D1BA 2D7B4E22 7EBDB816
        24732755 E6E1FBD4 05EA97CD 22E40D68 E96FF680 07412421

Z is
                                                    004355F7
        D66FE5C6 333D6C57 B6BD562D 25EA51F5 9D5EAFCC E6A17F78
        0A52FEC8 726E11F0 075AAD5E 33BA4106 ACEAD43D 8F294F18

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
        8909314B 9FA1C205 7F624010 8F62526B 6B3268FE 2C3F0E74
        53D16A7A 9B0DA0B3 F27B46B3 58E0D979 9DBE02FF 28E1F588
        29B4DCD4 7996CA03 2805271A 2FBFF363 E9C83263 D73C0B71
        13004EA6 5FE549D7 56B6F624 6FFC4FB0 39CAAD10 E4FBD96E
        F2E4D022 F5A9ED57 932707B6 7F5C182D E9008AB5 EF9CEFE5

U2V

```
MacData is
                                                        4B435F32
        5F55414C 49434542 4F424259 00BDA188 5B7E54B3 66D5BEC1
        D652ECA6 1A395378 916541C7 935B09DB 557BC6EE 5E25FD9B
        BD77F039 D95ED6E9 4248FB03 B5655B44 01A7E08C BA0374A2
        C0AEFAFC 41608CF1 7E718888 DCE2132E 191F4565 15EFC4B7
        8C22E6B8 926C30F0 B513107B B88ABC84 FB15E337 0010F0B2
        F19A11B5 B520AC95 8B15B47F 40A0D1BA 2D7B4E22 7EBDB816
        24732755 E6E1FBD4 05EA97CD 22E40D68 E96FF680 07412421


MacKey is
        8909314B 9FA1C205 7F624010 8F62526B 6B3268FE 2C3F0E74


Mtag is
        924CCD04 66CBA124 CA6796CA 3D9041D2 6FBFD5F4 5F1EE4C1
        5F8F1BAC 75A502B7 3B98000D FE25F52D 173D3485 95647E21


V2U
----------------
MacData is
                                                        4B435F32
        5F56424F 42425941 4C494345 0010F0B2 F19A11B5 B520AC95
        8B15B47F 40A0D1BA 2D7B4E22 7EBDB816 24732755 E6E1FBD4
        05EA97CD 22E40D68 E96FF680 07412421 00BDA188 5B7E54B3
        66D5BEC1 D652ECA6 1A395378 916541C7 935B09DB 557BC6EE
        5E25FD9B BD77F039 D95ED6E9 4248FB03 B5655B44 01A7E08C
        BA0374A2 C0AEFAFC 41608CF1 7E718888 DCE2132E 191F4565
        15EFC4B7 8C22E6B8 926C30F0 B513107B B88ABC84 FB15E337


MacKey is
        8909314B 9FA1C205 7F624010 8F62526B 6B3268FE 2C3F0E74


Mtag is
        1A85D188 4F500FD2 1E113AB4 EA1E7A68 1C6DE02F DDFB5202
        5E58D382 1EE1E0E7 22E86E4E 06CE6A29 D3C814BD D40EED51


KeyData is
        53D16A7A 9B0DA0B3 F27B46B3 58E0D979 9DBE02FF 28E1F588
        29B4DCD4 7996CA03 2805271A 2FBFF363 E9C83263 D73C0B71
        13004EA6 5FE549D7 56B6F624 6FFC4FB0 39CAAD10 E4FBD96E
```

F2E4D022 F5A9ED57 932707B6 7F5C182D E9008AB5 EF9CEFE5

OnePassDiffieHellmanCDH(K-409)
---
dsV is
0047F7DF
0EB84625 BFE69F8C 9DE845AF A5A26EDD C41B6B56 47360A53
71398245 8EA0231A F2DA0BAE FA71EB6C 05E1B7D0 837BBFA1

QsV_x is
0107C00B
AB1A1085 9172E54E B34DC8BE 22ECCAF9 08E65F4E B97BF481
F86C0B15 DB869112 8CABD886 9CDDC529 B48AFF82 819A79D0

QsV_y is
01321631
46FF3175 E33C5B4F 528BD187 1895B9B9 C01762EB 96CE6E8C
B20B8CA7 D476D85D 35D7893C 98D5F24D 7E63CBA2 A9608156

deU is
006EF9F6
34D00E22 A3876CBA 3732D0C9 5B3DD356 855E319B 299DFF89
D5D6FDC4 23C76085 CC5FFB50 D2F8DE27 37B56616 9C5A63B4

QeU_x is
00BDA188
5B7E54B3 66D5BEC1 D652ECA6 1A395378 916541C7 935B09DB
557BC6EE 5E25FD9B BD77F039 D95ED6E9 4248FB03 B5655B44

QeU_y is
01A7E08C
BA0374A2 C0AEFAFC 41608CF1 7E718888 DCE2132E 191F4565
15EFC4B7 8C22E6B8 926C30F0 B513107B B88ABC84 FB15E337

---

no Key Confirmation
Z is
                                                        000AD809
        4E7EA41A 4EC724DC B2621062 C0BEAE30 71A83480 C7357E40
        91468F86 7B5EDE0E 0D2ECB8A ED3A8463 C91E1F82 A855D0A2

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
        B4AD0592 240BF946 E9254491 B75CC5C3 6692C103 AE35791D
        3052DCF3 333311B0 44A26FE2 CE9BBB26 37CB77D2 9910D054
        E1FE47B5 CD7A9AA7 25B765DF F45E1120 4BFEF351 81EF32D8
        DB5787C8 B80AFE67 F5B7121D 3EC6E5F5 C8FE96D0 B1E882AC

KeyData is
        B4AD0592 240BF946 E9254491 B75CC5C3 6692C103 AE35791D
        3052DCF3 333311B0 44A26FE2 CE9BBB26 37CB77D2 9910D054
        E1FE47B5 CD7A9AA7 25B765DF F45E1120 4BFEF351 81EF32D8
        DB5787C8 B80AFE67 F5B7121D 3EC6E5F5 C8FE96D0 B1E882AC

Scheme Responder, Key Confirmation Provider: V to U
Z is
                                                        000AD809
        4E7EA41A 4EC724DC B2621062 C0BEAE30 71A83480 C7357E40
        91468F86 7B5EDE0E 0D2ECB8A ED3A8463 C91E1F82 A855D0A2

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
        B4AD0592 240BF946 E9254491 B75CC5C3 6692C103 AE35791D
        3052DCF3 333311B0 44A26FE2 CE9BBB26 37CB77D2 9910D054
        E1FE47B5 CD7A9AA7 25B765DF F45E1120 4BFEF351 81EF32D8
        DB5787C8 B80AFE67 F5B7121D 3EC6E5F5 C8FE96D0 B1E882AC
        D2BCFC00 154E5133 A25399D0 C0A8E636 FE26FFDA B7EF403D

MacData is
        4B435F31 5F56424F 42425941 4C494345 00BDA188 5B7E54B3
        66D5BEC1 D652ECA6 1A395378 916541C7 935B09DB 557BC6EE
        5E25FD9B BD77F039 D95ED6E9 4248FB03 B5655B44 01A7E08C
        BA0374A2 C0AEFAFC 41608CF1 7E718888 DCE2132E 191F4565
        15EFC4B7 8C22E6B8 926C30F0 B513107B B88ABC84 FB15E337

MacKey is
        B4AD0592 240BF946 E9254491 B75CC5C3 6692C103 AE35791D

Mtag is
        63AC6BC8 0531A806 B27870EA 88E10E27 92189C11 05566DD2
        D634C2D0 4BD102C0 03D2EA75 98483AEF B968AC6A 900E8E61

KeyData is
        3052DCF3 333311B0 44A26FE2 CE9BBB26 37CB77D2 9910D054
        E1FE47B5 CD7A9AA7 25B765DF F45E1120 4BFEF351 81EF32D8
        DB5787C8 B80AFE67 F5B7121D 3EC6E5F5 C8FE96D0 B1E882AC
        D2BCFC00 154E5133 A25399D0 C0A8E636 FE26FFDA B7EF403D

StaticUnifiedCDH(K-409)
----
dsU is
                                                    000D579E
        CEE513ED F7095D2B 5D7F0493 D43E586A BA5DC476 BC164F2A
        EAFA3DFC 05AF1BD5 81E9F515 97EC437D 2ABE947B 2D86ABEE

QsU_x is
                                                    0057825B
        87F2BD5D 76A67091 72DE78BC FE0EEFF1 502E502A 7F439D99
        8A5C7674 6379120B A97BD749 0F1BD4E4 569A5F92 94E7A6E4

QsU_y is
                                                    010B4376
        B99CAB68 9D3D085A A09B7D3A 4B340804 DCFD680D B474F8C6
        466EC971 C2FD710F 81B80924 9AFD78D1 2D45754A 0BAD530D

```
dsV is
                                                        00380820
        F149F869 BB0510E4 E2C82E6C 279B2F31 7BAF6FF6 BC42EF45
        A4784A13 4A5879FD D6A5975E 88D7089A 348D5942 F329E352


QsV_x is
                                                        00EF1E1C
        F8DD2883 45617868 19C7BDAF D4B609AE 8B8E0DBB 9AD38FA1
        550AEF08 840F1B6F 612BE777 C952AC69 E3F51291 C75EB91A


QsV_y is
                                                        01C3608C
        E8DBD74E 77DFD109 7F6E47E6 FCD743DC E6192FA7 DCB8810D
        DECAC13E 81A9527E 640B7ED8 33D7F416 D51BC84D 7497AC51




------------------------------------------------------------
no Key Confirmation
NonceU is
                                                        0010F0B2
        F19A11B5 B520AC95 8B15B47F 40A0D1BA 2D7B4E22 7EBDB816
        24732755 E6E1FBD4 05EA97CD 22E40D68 E96FF680 07412421


Z is
                                                        0120F46D
        9195B260 528840E5 EF902C4F 03208AAF EBC94CE2 08ED6974
        84FEF3A7 6BF293F1 9853540A 2F35C3C3 6B5F04CC D2B7FE5C


OtherInfo is
                                                    1234 56789ABC
        DEF0414C 49434531 32339901 0010F0B2 F19A11B5 B520AC95
        8B15B47F 40A0D1BA 2D7B4E22 7EBDB816 24732755 E6E1FBD4
        05EA97CD 22E40D68 E96FF680 07412421 424F4242 59343536


DerivedKeyMaterial is
        5A49AA59 4322A40A 27EE0FB0 EC4E1CFA 28B6DEF8 BA88ED89
        3EE625FE 60E4219F 0838A7D6 5F48A756 228902F1 A6DFD1BE
        8EB8D229 3B3B51A7 109D5C35 81EC5F60 309815D2 1105AFD1
```

```
        321D604C 28F89229 45031E61 377E12E6 C2F98DA2 70A8B626


KeyData is
        5A49AA59 4322A40A 27EE0FB0 EC4E1CFA 28B6DEF8 BA88ED89
        3EE625FE 60E4219F 0838A7D6 5F48A756 228902F1 A6DFD1BE
        8EB8D229 3B3B51A7 109D5C35 81EC5F60 309815D2 1105AFD1
        321D604C 28F89229 45031E61 377E12E6 C2F98DA2 70A8B626




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceU is
                                                    0010F0B2
        F19A11B5 B520AC95 8B15B47F 40A0D1BA 2D7B4E22 7EBDB816
        24732755 E6E1FBD4 05EA97CD 22E40D68 E96FF680 07412421


NonceV is
                                                    002B5F06
        5A4650B5 2FACE92F 084CE8C7 1949990B 68350696 E8C529BF
        BA58E8B6 CF0BB21C 6E1F1AB8 C2D6F34F 124D2AF6 6F402478


Z is
                                                    0120F46D
        9195B260 528840E5 EF902C4F 03208AAF EBC94CE2 08ED6974
        84FEF3A7 6BF293F1 9853540A 2F35C3C3 6B5F04CC D2B7FE5C


OtherInfo is
                                                1234 56789ABC
        DEF0414C 49434531 32339901 0010F0B2 F19A11B5 B520AC95
        8B15B47F 40A0D1BA 2D7B4E22 7EBDB816 24732755 E6E1FBD4
        05EA97CD 22E40D68 E96FF680 07412421 424F4242 59343536


DerivedKeyMaterial is
        5A49AA59 4322A40A 27EE0FB0 EC4E1CFA 28B6DEF8 BA88ED89
        3EE625FE 60E4219F 0838A7D6 5F48A756 228902F1 A6DFD1BE
        8EB8D229 3B3B51A7 109D5C35 81EC5F60 309815D2 1105AFD1
        321D604C 28F89229 45031E61 377E12E6 C2F98DA2 70A8B626
        0DCB539A 067C39CF 39C42FB8 BC87B25D B60FF0A9 B3F547F5
```

MacData is
4B435F31 5F55414C 49434542 4F424259 0010F0B2 F19A11B5
B520AC95 8B15B47F 40A0D1BA 2D7B4E22 7EBDB816 24732755
E6E1FBD4 05EA97CD 22E40D68 E96FF680 07412421 002B5F06
5A4650B5 2FACE92F 084CE8C7 1949990B 68350696 E8C529BF
BA58E8B6 CF0BB21C 6E1F1AB8 C2D6F34F 124D2AF6 6F402478

MacKey is
5A49AA59 4322A40A 27EE0FB0 EC4E1CFA 28B6DEF8 BA88ED89

Mtag is
EA03EA60 3EA72435 356A45C6 869C27A6 31D95C04 440F9B88
4BC4ADB1 FA5CC93F 45913D8B A5256E6E 6245E222 98351E81

KeyData is
3EE625FE 60E4219F 0838A7D6 5F48A756 228902F1 A6DFD1BE
8EB8D229 3B3B51A7 109D5C35 81EC5F60 309815D2 1105AFD1
321D604C 28F89229 45031E61 377E12E6 C2F98DA2 70A8B626
0DCB539A 067C39CF 39C42FB8 BC87B25D B60FF0A9 B3F547F5

Scheme Responder, Key Confirmation Provider: V to U
NonceV is
002B5F06
5A4650B5 2FACE92F 084CE8C7 1949990B 68350696 E8C529BF
BA58E8B6 CF0BB21C 6E1F1AB8 C2D6F34F 124D2AF6 6F402478

NonceU is
0010F0B2
F19A11B5 B520AC95 8B15B47F 40A0D1BA 2D7B4E22 7EBDB816
24732755 E6E1FBD4 05EA97CD 22E40D68 E96FF680 07412421

Z is
0120F46D
9195B260 528840E5 EF902C4F 03208AAF EBC94CE2 08ED6974
84FEF3A7 6BF293F1 9853540A 2F35C3C3 6B5F04CC D2B7FE5C

```
OtherInfo is
                                                    1234 56789ABC
        DEF0414C 49434531 32339901 0010F0B2 F19A11B5 B520AC95
        8B15B47F 40A0D1BA 2D7B4E22 7EBDB816 24732755 E6E1FBD4
        05EA97CD 22E40D68 E96FF680 07412421 424F4242 59343536


DerivedKeyMaterial is
        5A49AA59 4322A40A 27EE0FB0 EC4E1CFA 28B6DEF8 BA88ED89
        3EE625FE 60E4219F 0838A7D6 5F48A756 228902F1 A6DFD1BE
        8EB8D229 3B3B51A7 109D5C35 81EC5F60 309815D2 1105AFD1
        321D604C 28F89229 45031E61 377E12E6 C2F98DA2 70A8B626
        0DCB539A 067C39CF 39C42FB8 BC87B25D B60FF0A9 B3F547F5


MacData is
                 4B435F31 5F56424F 42425941 4C494345 0010F0B2
        F19A11B5 B520AC95 8B15B47F 40A0D1BA 2D7B4E22 7EBDB816
        24732755 E6E1FBD4 05EA97CD 22E40D68 E96FF680 07412421


MacKey is
        5A49AA59 4322A40A 27EE0FB0 EC4E1CFA 28B6DEF8 BA88ED89


Mtag is
        3CA57348 AE14A76C A8AA2CB7 3F15A180 850C0046 F8BFF80F
        92F9E486 0CE9D2AA FFEBC3E0 227FBBE8 EC0E23B3 9E3A4C26


KeyData is
        3EE625FE 60E4219F 0838A7D6 5F48A756 228902F1 A6DFD1BE
        8EB8D229 3B3B51A7 109D5C35 81EC5F60 309815D2 1105AFD1
        321D604C 28F89229 45031E61 377E12E6 C2F98DA2 70A8B626
        0DCB539A 067C39CF 39C42FB8 BC87B25D B60FF0A9 B3F547F5




------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
NonceU is
                                                        0010F0B2
        F19A11B5 B520AC95 8B15B47F 40A0D1BA 2D7B4E22 7EBDB816
```

```
        24732755 E6E1FBD4 05EA97CD 22E40D68 E96FF680 07412421


NonceV is
                                                        002B5F06
        5A4650B5 2FACE92F 084CE8C7 1949990B 68350696 E8C529BF
        BA58E8B6 CF0BB21C 6E1F1AB8 C2D6F34F 124D2AF6 6F402478


Z is
                                                        0120F46D
        9195B260 528840E5 EF902C4F 03208AAF EBC94CE2 08ED6974
        84FEF3A7 6BF293F1 9853540A 2F35C3C3 6B5F04CC D2B7FE5C


OtherInfo is
                                                    1234 56789ABC
        DEF0414C 49434531 32339901 0010F0B2 F19A11B5 B520AC95
        8B15B47F 40A0D1BA 2D7B4E22 7EBDB816 24732755 E6E1FBD4
        05EA97CD 22E40D68 E96FF680 07412421 424F4242 59343536


DerivedKeyMaterial is
        5A49AA59 4322A40A 27EE0FB0 EC4E1CFA 28B6DEF8 BA88ED89
        3EE625FE 60E4219F 0838A7D6 5F48A756 228902F1 A6DFD1BE
        8EB8D229 3B3B51A7 109D5C35 81EC5F60 309815D2 1105AFD1
        321D604C 28F89229 45031E61 377E12E6 C2F98DA2 70A8B626
        0DCB539A 067C39CF 39C42FB8 BC87B25D B60FF0A9 B3F547F5


U2V
----------------
MacData is
        4B435F32 5F55414C 49434542 4F424259 0010F0B2 F19A11B5
        B520AC95 8B15B47F 40A0D1BA 2D7B4E22 7EBDB816 24732755
        E6E1FBD4 05EA97CD 22E40D68 E96FF680 07412421 002B5F06
        5A4650B5 2FACE92F 084CE8C7 1949990B 68350696 E8C529BF
        BA58E8B6 CF0BB21C 6E1F1AB8 C2D6F34F 124D2AF6 6F402478


MacKey is
        5A49AA59 4322A40A 27EE0FB0 EC4E1CFA 28B6DEF8 BA88ED89


Mtag is
        D621C5CC EDF6D4BD 43B1CED4 C89FBE45 9F916A59 6F81AA6C
```

8FB5D9DD 3208E4B6 1BAD93BC 8DC899D2 54BBC1FF F653203D

V2U

MacData is
4B435F32 5F56424F 42425941 4C494345 002B5F06 5A4650B5
2FACE92F 084CE8C7 1949990B 68350696 E8C529BF BA58E8B6
CF0BB21C 6E1F1AB8 C2D6F34F 124D2AF6 6F402478 0010F0B2
F19A11B5 B520AC95 8B15B47F 40A0D1BA 2D7B4E22 7EBDB816
24732755 E6E1FBD4 05EA97CD 22E40D68 E96FF680 07412421

MacKey is
5A49AA59 4322A40A 27EE0FB0 EC4E1CFA 28B6DEF8 BA88ED89

Mtag is
33502EC2 65B61392 63B7CB99 05E53013 8E86F0B6 C472DB8F
DC9519BE 1FDAA180 E2FC80DF 76E9C155 089E9AD6 63917EC8

KeyData is
3EE625FE 60E4219F 0838A7D6 5F48A756 228902F1 A6DFD1BE
8EB8D229 3B3B51A7 109D5C35 81EC5F60 309815D2 1105AFD1
321D604C 28F89229 45031E61 377E12E6 C2F98DA2 70A8B626
0DCB539A 067C39CF 39C42FB8 BC87B25D B60FF0A9 B3F547F5

```
FullUnifiedCDH(B-409)
------------------------------------------------------------
dsU is
                                                        00F2A861
        311B086F 575FC709 16F04E30 44FB4CA3 12C352FF 0C12ED4A
        AB990E1B 8D929967 BD55C76D 03390257 5969437E 73A68381


QsU_x is
                                                        01EFFB75
        A8476005 0D112FA8 05106512 2D9A24EF 28FDD510 91E94FD3
        E868F036 5063DC0C CAF6D734 2CBEED5C F69C835B 681E6B43


QsU_y is
                                                        005A8E93
        A6E264AC CB9862FB 3ECF72D1 97E509CC 850FAE8E 76D33FD2
        8FD45E95 459D68E0 9C42097C 2750995B 19846B2D 02EA425F


dsV is
                                                        0047F7DF
        0EB6F57C 05B83D7F 7AD60D30 F1134508 F305AD88 7CA2850A
        9E2AE76D 366CD506 AA90E9DA 3D184122 31ED33A0 280A5792


QsV_x is
                                                        0138DF61
        834D9C39 AA3B157B 263AB64C 570239BB 6DD4120B A8E3F13D
        E3CE17C5 5B87A655 20577E88 9B9BB7E3 190E095E C551A53D


QsV_y is
                                                        007FF7B7
        79B76892 2E13A3DF AABDF60F 056B6F6D 2F2EEEE8 C0CB50AE
        F0816E5A 21EE4E6A FC6E75FD F532CEA6 EA4F99DF DAC6BF32


deU is
                                                        006EF9F6
        34CCE619 5CBF086A 40C58EB4 EAD07416 BD901E5C 3705EC7F
        9231DB0C A2A6020A FBD992AB 6698B1A3 ABBEF462 A1ADBC84
```

QeU_x is

01FA5D9C
C2DBC999 B55354A4 F921FC42 19D334D4 F71CD68E B19220A1
D20D829D 95FB8785 A30A0B59 562FB7E9 250CD095 0B80C397

QeU_y is

01D71C9F
78D4C735 40C4F606 26400F43 5D0BB59C 579E0BF8 7475620F
0CFB6D3F 89F27C8D 0A9C2A40 BED5D71C 10ED6C99 9FBDB3B7

deV is

0027B021
03600E10 CBAF0D99 A01A3C19 B56C2D05 2693A382 07677E5B
1149CE1A 146AA137 D0C9524E 199D5CE3 432B05A2 131ECB50

QeV_x is

01D325B4
1C395BF7 31500C87 1043A032 6F4CA12D 8B124FD6 C17A13B5
246C220B DA903A84 8AE6682F FF4BF764 874E06D9 8FBABC29

QeV_y is

0116CD16
69FBE8BD CC7A1DA6 D9D88055 EDDF361C DF245140 0B65D868
1DCA400F 5332374B 4E65EB36 2B3CD612 40C1FCA8 7CC7D8A4

---

no Key Confirmation
Zs is

00494A68
E6BF47C7 7402FF79 82950101 E92F2D78 C7A59A85 ACF56F11
57F28B49 8DAB7392 C933B149 54D54F88 8355B87A 80B16E8D

Ze is

0006FAD8
492E08DE 6B2F938B A5B6BA28 1E995EEC D540D788 6BD6EAA3
7E6C1FC5 3EAA5B33 65DFEA24 35082CFC C68BF9E3 2A53E641

```
Z is
                                                0006FAD8 492E08DE
        6B2F938B A5B6BA28 1E995EEC D540D788 6BD6EAA3 7E6C1FC5
        3EAA5B33 65DFEA24 35082CFC C68BF9E3 2A53E641 00494A68
        E6BF47C7 7402FF79 82950101 E92F2D78 C7A59A85 ACF56F11
        57F28B49 8DAB7392 C933B149 54D54F88 8355B87A 80B16E8D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        78A40A27 9F0A8417 0C7DC2F4 26143032 FFEAF82C 26AB9A68
        BF4552B2 B374393D 26439F94 FD0B87C7 A28915C1 9716D485
        BB1052AC 9D9D5947 9507C3A7 18E0F45E 01F30FC4 62DECFBD
        222B9383 9226BE0B E5A87876 7C432CC2 58DEF448 12B985DD


KeyData is
        78A40A27 9F0A8417 0C7DC2F4 26143032 FFEAF82C 26AB9A68
        BF4552B2 B374393D 26439F94 FD0B87C7 A28915C1 9716D485
        BB1052AC 9D9D5947 9507C3A7 18E0F45E 01F30FC4 62DECFBD
        222B9383 9226BE0B E5A87876 7C432CC2 58DEF448 12B985DD




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Zs is
                                                    00494A68
        E6BF47C7 7402FF79 82950101 E92F2D78 C7A59A85 ACF56F11
        57F28B49 8DAB7392 C933B149 54D54F88 8355B87A 80B16E8D


Ze is
                                                    0006FAD8
        492E08DE 6B2F938B A5B6BA28 1E995EEC D540D788 6BD6EAA3
        7E6C1FC5 3EAA5B33 65DFEA24 35082CFC C68BF9E3 2A53E641


Z is
                                                0006FAD8 492E08DE
        6B2F938B A5B6BA28 1E995EEC D540D788 6BD6EAA3 7E6C1FC5
        3EAA5B33 65DFEA24 35082CFC C68BF9E3 2A53E641 00494A68
```

```
        E6BF47C7 7402FF79 82950101 E92F2D78 C7A59A85 ACF56F11
        57F28B49 8DAB7392 C933B149 54D54F88 8355B87A 80B16E8D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        78A40A27 9F0A8417 0C7DC2F4 26143032 FFEAF82C 26AB9A68
        BF4552B2 B374393D 26439F94 FD0B87C7 A28915C1 9716D485
        BB1052AC 9D9D5947 9507C3A7 18E0F45E 01F30FC4 62DECFBD
        222B9383 9226BE0B E5A87876 7C432CC2 58DEF448 12B985DD
        B7C6A22A C2B87AFC BE1E3EF0 EA72200E 3AB75112 EA6D316B


MacData is
                                            4B435F31 5F55414C
        49434542 4F424259 01FA5D9C C2DBC999 B55354A4 F921FC42
        19D334D4 F71CD68E B19220A1 D20D829D 95FB8785 A30A0B59
        562FB7E9 250CD095 0B80C397 01D71C9F 78D4C735 40C4F606
        26400F43 5D0BB59C 579E0BF8 7475620F 0CFB6D3F 89F27C8D
        0A9C2A40 BED5D71C 10ED6C99 9FBDB3B7 01D325B4 1C395BF7
        31500C87 1043A032 6F4CA12D 8B124FD6 C17A13B5 246C220B
        DA903A84 8AE6682F FF4BF764 874E06D9 8FBABC29 0116CD16
        69FBE8BD CC7A1DA6 D9D88055 EDDF361C DF245140 0B65D868
        1DCA400F 5332374B 4E65EB36 2B3CD612 40C1FCA8 7CC7D8A4


MacKey is
        78A40A27 9F0A8417 0C7DC2F4 26143032 FFEAF82C 26AB9A68


Mtag is
        B428FCC1 12673881 38486B81 BE311863 4CB5758B 5AA8B382
        30DE86DA EB726797 DE878457 432BC917 2291DAD9 7C76F7A2


KeyData is
        BF4552B2 B374393D 26439F94 FD0B87C7 A28915C1 9716D485
        BB1052AC 9D9D5947 9507C3A7 18E0F45E 01F30FC4 62DECFBD
        222B9383 9226BE0B E5A87876 7C432CC2 58DEF448 12B985DD
        B7C6A22A C2B87AFC BE1E3EF0 EA72200E 3AB75112 EA6D316B
```

```
------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Zs is
                                                        00494A68
        E6BF47C7 7402FF79 82950101 E92F2D78 C7A59A85 ACF56F11
        57F28B49 8DAB7392 C933B149 54D54F88 8355B87A 80B16E8D


Ze is
                                                        0006FAD8
        492E08DE 6B2F938B A5B6BA28 1E995EEC D540D788 6BD6EAA3
        7E6C1FC5 3EAA5B33 65DFEA24 35082CFC C68BF9E3 2A53E641


Z is
                                                0006FAD8 492E08DE
        6B2F938B A5B6BA28 1E995EEC D540D788 6BD6EAA3 7E6C1FC5
        3EAA5B33 65DFEA24 35082CFC C68BF9E3 2A53E641 00494A68
        E6BF47C7 7402FF79 82950101 E92F2D78 C7A59A85 ACF56F11
        57F28B49 8DAB7392 C933B149 54D54F88 8355B87A 80B16E8D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        78A40A27 9F0A8417 0C7DC2F4 26143032 FFEAF82C 26AB9A68
        BF4552B2 B374393D 26439F94 FD0B87C7 A28915C1 9716D485
        BB1052AC 9D9D5947 9507C3A7 18E0F45E 01F30FC4 62DECFBD
        222B9383 9226BE0B E5A87876 7C432CC2 58DEF448 12B985DD
        B7C6A22A C2B87AFC BE1E3EF0 EA72200E 3AB75112 EA6D316B


MacData is
                                                4B435F31 5F56424F
        42425941 4C494345 01D325B4 1C395BF7 31500C87 1043A032
        6F4CA12D 8B124FD6 C17A13B5 246C220B DA903A84 8AE6682F
        FF4BF764 874E06D9 8FBABC29 0116CD16 69FBE8BD CC7A1DA6
        D9D88055 EDDF361C DF245140 0B65D868 1DCA400F 5332374B
        4E65EB36 2B3CD612 40C1FCA8 7CC7D8A4 01FA5D9C C2DBC999
        B55354A4 F921FC42 19D334D4 F71CD68E B19220A1 D20D829D
        95FB8785 A30A0B59 562FB7E9 250CD095 0B80C397 01D71C9F
        78D4C735 40C4F606 26400F43 5D0BB59C 579E0BF8 7475620F
        0CFB6D3F 89F27C8D 0A9C2A40 BED5D71C 10ED6C99 9FBDB3B7
```

```
MacKey is
        78A40A27 9F0A8417 0C7DC2F4 26143032 FFEAF82C 26AB9A68


Mtag is
        7989E67B FDB3F0AB EE74CBD4 8B5BD568 76963579 E5DC538A
        26ADC31A 695AF3E9 AAE621D7 3206EA5B 202772ED 525D1558


KeyData is
        BF4552B2 B374393D 26439F94 FD0B87C7 A28915C1 9716D485
        BB1052AC 9D9D5947 9507C3A7 18E0F45E 01F30FC4 62DECFBD
        222B9383 9226BE0B E5A87876 7C432CC2 58DEF448 12B985DD
        B7C6A22A C2B87AFC BE1E3EF0 EA72200E 3AB75112 EA6D316B




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
Zs is
                                                    00494A68
        E6BF47C7 7402FF79 82950101 E92F2D78 C7A59A85 ACF56F11
        57F28B49 8DAB7392 C933B149 54D54F88 8355B87A 80B16E8D


Ze is
                                                    0006FAD8
        492E08DE 6B2F938B A5B6BA28 1E995EEC D540D788 6BD6EAA3
        7E6C1FC5 3EAA5B33 65DFEA24 35082CFC C68BF9E3 2A53E641


Z is
                                            0006FAD8 492E08DE
        6B2F938B A5B6BA28 1E995EEC D540D788 6BD6EAA3 7E6C1FC5
        3EAA5B33 65DFEA24 35082CFC C68BF9E3 2A53E641 00494A68
        E6BF47C7 7402FF79 82950101 E92F2D78 C7A59A85 ACF56F11
        57F28B49 8DAB7392 C933B149 54D54F88 8355B87A 80B16E8D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536
```

```
DerivedKeyMaterial is
        78A40A27 9F0A8417 0C7DC2F4 26143032 FFEAF82C 26AB9A68
        BF4552B2 B374393D 26439F94 FD0B87C7 A28915C1 9716D485
        BB1052AC 9D9D5947 9507C3A7 18E0F45E 01F30FC4 62DECFBD
        222B9383 9226BE0B E5A87876 7C432CC2 58DEF448 12B985DD
        B7C6A22A C2B87AFC BE1E3EF0 EA72200E 3AB75112 EA6D316B


U2V
----------------
MacData is
                                            4B435F32 5F55414C
        49434542 4F424259 01FA5D9C C2DBC999 B55354A4 F921FC42
        19D334D4 F71CD68E B19220A1 D20D829D 95FB8785 A30A0B59
        562FB7E9 250CD095 0B80C397 01D71C9F 78D4C735 40C4F606
        26400F43 5D0BB59C 579E0BF8 7475620F 0CFB6D3F 89F27C8D
        0A9C2A40 BED5D71C 10ED6C99 9FBDB3B7 01D325B4 1C395BF7
        31500C87 1043A032 6F4CA12D 8B124FD6 C17A13B5 246C220B
        DA903A84 8AE6682F FF4BF764 874E06D9 8FBABC29 0116CD16
        69FBE8BD CC7A1DA6 D9D88055 EDDF361C DF245140 0B65D868
        1DCA400F 5332374B 4E65EB36 2B3CD612 40C1FCA8 7CC7D8A4


MacKey is
        78A40A27 9F0A8417 0C7DC2F4 26143032 FFEAF82C 26AB9A68


Mtag is
        9168FDAA CD360F0A 75B00B3E 7C6A56C8 C182646F 3491B9B3
        BA932162 76CF9FF6 82532971 E359C10B B6E42805 2ADB4E0A


V2U
----------------
MacData is
                                            4B435F32 5F56424F
        42425941 4C494345 01D325B4 1C395BF7 31500C87 1043A032
        6F4CA12D 8B124FD6 C17A13B5 246C220B DA903A84 8AE6682F
        FF4BF764 874E06D9 8FBABC29 0116CD16 69FBE8BD CC7A1DA6
        D9D88055 EDDF361C DF245140 0B65D868 1DCA400F 5332374B
        4E65EB36 2B3CD612 40C1FCA8 7CC7D8A4 01FA5D9C C2DBC999
        B55354A4 F921FC42 19D334D4 F71CD68E B19220A1 D20D829D
        95FB8785 A30A0B59 562FB7E9 250CD095 0B80C397 01D71C9F
        78D4C735 40C4F606 26400F43 5D0BB59C 579E0BF8 7475620F
        0CFB6D3F 89F27C8D 0A9C2A40 BED5D71C 10ED6C99 9FBDB3B7
```

MacKey is
        78A40A27 9F0A8417 0C7DC2F4 26143032 FFEAF82C 26AB9A68

Mtag is
        9422787C 2DB41E3A 8E853AC6 0DFE061C 17E5B279 0A65BD9D
        8EB1BFB7 30581EC8 C1442265 C43FD856 7FE45F2A 47700326

KeyData is
        BF4552B2 B374393D 26439F94 FD0B87C7 A28915C1 9716D485
        BB1052AC 9D9D5947 9507C3A7 18E0F45E 01F30FC4 62DECFBD
        222B9383 9226BE0B E5A87876 7C432CC2 58DEF448 12B985DD
        B7C6A22A C2B87AFC BE1E3EF0 EA72200E 3AB75112 EA6D316B

FullMQV(B-409)
---
dsU is
                                                        00F2A861
        311B086F 575FC709 16F04E30 44FB4CA3 12C352FF 0C12ED4A
        AB990E1B 8D929967 BD55C76D 03390257 5969437E 73A68381

QsU_x is
                                                        01EFFB75
        A8476005 0D112FA8 05106512 2D9A24EF 28FDD510 91E94FD3
        E868F036 5063DC0C CAF6D734 2CBEED5C F69C835B 681E6B43

QsU_y is
                                                        005A8E93
        A6E264AC CB9862FB 3ECF72D1 97E509CC 850FAE8E 76D33FD2
        8FD45E95 459D68E0 9C42097C 2750995B 19846B2D 02EA425F

dsV is
                                                        0047F7DF
        0EB6F57C 05B83D7F 7AD60D30 F1134508 F305AD88 7CA2850A
        9E2AE76D 366CD506 AA90E9DA 3D184122 31ED33A0 280A5792

QsV_x is

```
                                                        0138DF61
        834D9C39 AA3B157B 263AB64C 570239BB 6DD4120B A8E3F13D
        E3CE17C5 5B87A655 20577E88 9B9BB7E3 190E095E C551A53D


QsV_y is
                                                        007FF7B7
        79B76892 2E13A3DF AABDF60F 056B6F6D 2F2EEEE8 C0CB50AE
        F0816E5A 21EE4E6A FC6E75FD F532CEA6 EA4F99DF DAC6BF32


deU is
                                                        006EF9F6
        34CCE619 5CBF086A 40C58EB4 EAD07416 BD901E5C 3705EC7F
        9231DB0C A2A6020A FBD992AB 6698B1A3 ABBEF462 A1ADBC84


QeU_x is
                                                        01FA5D9C
        C2DBC999 B55354A4 F921FC42 19D334D4 F71CD68E B19220A1
        D20D829D 95FB8785 A30A0B59 562FB7E9 250CD095 0B80C397


QeU_y is
                                                        01D71C9F
        78D4C735 40C4F606 26400F43 5D0BB59C 579E0BF8 7475620F
        0CFB6D3F 89F27C8D 0A9C2A40 BED5D71C 10ED6C99 9FBDB3B7


deV is
                                                        0027B021
        03600E10 CBAF0D99 A01A3C19 B56C2D05 2693A382 07677E5B
        1149CE1A 146AA137 D0C9524E 199D5CE3 432B05A2 131ECB50


QeV_x is
                                                        01D325B4
        1C395BF7 31500C87 1043A032 6F4CA12D 8B124FD6 C17A13B5
        246C220B DA903A84 8AE6682F FF4BF764 874E06D9 8FBABC29


QeV_y is
                                                        0116CD16
        69FBE8BD CC7A1DA6 D9D88055 EDDF361C DF245140 0B65D868
        1DCA400F 5332374B 4E65EB36 2B3CD612 40C1FCA8 7CC7D8A4
```

```
-----------------------------------------------------------
no Key Confirmation
Z is
                                                      010D3116
        14BBEE06 8AC7A2EF 08036B71 4594CA75 89F87DC1 C55B4328
        E5CFC845 B065337D F9CABA86 8614FC23 3BDDE388 A9C1C997


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        3D4C2DF7 DCEDD76A 9A744D98 265C64BE 518214D7 CF0C80BE
        E264E3D0 BD3CD563 355ACD02 9CF8E011 9EC24B62 C58D4AA7
        5F0DE506 BBF3982D 05383F41 B31778FE 235B7897 1F6448C3
        12BDE4D4 B3DE57FA 404F4C01 ACD2F1E2 78C41DB5 1350B550


KeyData is
        3D4C2DF7 DCEDD76A 9A744D98 265C64BE 518214D7 CF0C80BE
        E264E3D0 BD3CD563 355ACD02 9CF8E011 9EC24B62 C58D4AA7
        5F0DE506 BBF3982D 05383F41 B31778FE 235B7897 1F6448C3
        12BDE4D4 B3DE57FA 404F4C01 ACD2F1E2 78C41DB5 1350B550




-----------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Z is
                                                      010D3116
        14BBEE06 8AC7A2EF 08036B71 4594CA75 89F87DC1 C55B4328
        E5CFC845 B065337D F9CABA86 8614FC23 3BDDE388 A9C1C997


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        3D4C2DF7 DCEDD76A 9A744D98 265C64BE 518214D7 CF0C80BE
        E264E3D0 BD3CD563 355ACD02 9CF8E011 9EC24B62 C58D4AA7
```

```
        5F0DE506 BBF3982D 05383F41 B31778FE 235B7897 1F6448C3
        12BDE4D4 B3DE57FA 404F4C01 ACD2F1E2 78C41DB5 1350B550
        BB1F3657 C5AF67A2 235528E4 07B38283 3D1CB7CC 02A61D62


MacData is
                                            4B435F31 5F55414C
        49434542 4F424259 01FA5D9C C2DBC999 B55354A4 F921FC42
        19D334D4 F71CD68E B19220A1 D20D829D 95FB8785 A30A0B59
        562FB7E9 250CD095 0B80C397 01D71C9F 78D4C735 40C4F606
        26400F43 5D0BB59C 579E0BF8 7475620F 0CFB6D3F 89F27C8D
        0A9C2A40 BED5D71C 10ED6C99 9FBDB3B7 01D325B4 1C395BF7
        31500C87 1043A032 6F4CA12D 8B124FD6 C17A13B5 246C220B
        DA903A84 8AE6682F FF4BF764 874E06D9 8FBABC29 0116CD16
        69FBE8BD CC7A1DA6 D9D88055 EDDF361C DF245140 0B65D868
        1DCA400F 5332374B 4E65EB36 2B3CD612 40C1FCA8 7CC7D8A4


MacKey is
        3D4C2DF7 DCEDD76A 9A744D98 265C64BE 518214D7 CF0C80BE


Mtag is
        8CFE03F9 839647D4 FCF9000C 807A0E35 4869A248 9669362A
        5B7C27C9 6E8B2ADA 30F7E881 F71D1AFC 066AAE5B 6D222FAD


KeyData is
        E264E3D0 BD3CD563 355ACD02 9CF8E011 9EC24B62 C58D4AA7
        5F0DE506 BBF3982D 05383F41 B31778FE 235B7897 1F6448C3
        12BDE4D4 B3DE57FA 404F4C01 ACD2F1E2 78C41DB5 1350B550
        BB1F3657 C5AF67A2 235528E4 07B38283 3D1CB7CC 02A61D62




-------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
                                                    010D3116
        14BBEE06 8AC7A2EF 08036B71 4594CA75 89F87DC1 C55B4328
        E5CFC845 B065337D F9CABA86 8614FC23 3BDDE388 A9C1C997


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536
```

DerivedKeyMaterial is
        3D4C2DF7 DCEDD76A 9A744D98 265C64BE 518214D7 CF0C80BE
        E264E3D0 BD3CD563 355ACD02 9CF8E011 9EC24B62 C58D4AA7
        5F0DE506 BBF3982D 05383F41 B31778FE 235B7897 1F6448C3
        12BDE4D4 B3DE57FA 404F4C01 ACD2F1E2 78C41DB5 1350B550
        BB1F3657 C5AF67A2 235528E4 07B38283 3D1CB7CC 02A61D62

MacData is
                                                4B435F31 5F56424F
        42425941 4C494345 01D325B4 1C395BF7 31500C87 1043A032
        6F4CA12D 8B124FD6 C17A13B5 246C220B DA903A84 8AE6682F
        FF4BF764 874E06D9 8FBABC29 0116CD16 69FBE8BD CC7A1DA6
        D9D88055 EDDF361C DF245140 0B65D868 1DCA400F 5332374B
        4E65EB36 2B3CD612 40C1FCA8 7CC7D8A4 01FA5D9C C2DBC999
        B55354A4 F921FC42 19D334D4 F71CD68E B19220A1 D20D829D
        95FB8785 A30A0B59 562FB7E9 250CD095 0B80C397 01D71C9F
        78D4C735 40C4F606 26400F43 5D0BB59C 579E0BF8 7475620F
        0CFB6D3F 89F27C8D 0A9C2A40 BED5D71C 10ED6C99 9FBDB3B7

MacKey is
        3D4C2DF7 DCEDD76A 9A744D98 265C64BE 518214D7 CF0C80BE

Mtag is
        DAD6F524 A63792D3 6FFEAEE2 5CF8D4D9 D1B1B0B7 C32A3E53
        E824B778 107DEBA6 3F15BD98 1F502D04 AB8C3E1B 139E79DB

KeyData is
        E264E3D0 BD3CD563 355ACD02 9CF8E011 9EC24B62 C58D4AA7
        5F0DE506 BBF3982D 05383F41 B31778FE 235B7897 1F6448C3
        12BDE4D4 B3DE57FA 404F4C01 ACD2F1E2 78C41DB5 1350B550
        BB1F3657 C5AF67A2 235528E4 07B38283 3D1CB7CC 02A61D62

Scheme Initiator, Key Confirmation Bilateral
Z is
                                                        010D3116

```
        14BBEE06 8AC7A2EF 08036B71 4594CA75 89F87DC1 C55B4328
        E5CFC845 B065337D F9CABA86 8614FC23 3BDDE388 A9C1C997


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        3D4C2DF7 DCEDD76A 9A744D98 265C64BE 518214D7 CF0C80BE
        E264E3D0 BD3CD563 355ACD02 9CF8E011 9EC24B62 C58D4AA7
        5F0DE506 BBF3982D 05383F41 B31778FE 235B7897 1F6448C3
        12BDE4D4 B3DE57FA 404F4C01 ACD2F1E2 78C41DB5 1350B550
        BB1F3657 C5AF67A2 235528E4 07B38283 3D1CB7CC 02A61D62


U2V
----------------
MacData is
                                            4B435F32 5F55414C
        49434542 4F424259 01FA5D9C C2DBC999 B55354A4 F921FC42
        19D334D4 F71CD68E B19220A1 D20D829D 95FB8785 A30A0B59
        562FB7E9 250CD095 0B80C397 01D71C9F 78D4C735 40C4F606
        26400F43 5D0BB59C 579E0BF8 7475620F 0CFB6D3F 89F27C8D
        0A9C2A40 BED5D71C 10ED6C99 9FBDB3B7 01D325B4 1C395BF7
        31500C87 1043A032 6F4CA12D 8B124FD6 C17A13B5 246C220B
        DA903A84 8AE6682F FF4BF764 874E06D9 8FBABC29 0116CD16
        69FBE8BD CC7A1DA6 D9D88055 EDDF361C DF245140 0B65D868
        1DCA400F 5332374B 4E65EB36 2B3CD612 40C1FCA8 7CC7D8A4


MacKey is
        3D4C2DF7 DCEDD76A 9A744D98 265C64BE 518214D7 CF0C80BE


Mtag is
        D658973E EF761521 FC29C217 AAF23346 066FAE4B FD77086A
        740163EB 34FA2001 AB158910 7842CA38 CBB9A4D6 4E070D9B


V2U
----------------
MacData is
                                            4B435F32 5F56424F
        42425941 4C494345 01D325B4 1C395BF7 31500C87 1043A032
        6F4CA12D 8B124FD6 C17A13B5 246C220B DA903A84 8AE6682F
```

```
        FF4BF764 874E06D9 8FBABC29 0116CD16 69FBE8BD CC7A1DA6
        D9D88055 EDDF361C DF245140 0B65D868 1DCA400F 5332374B
        4E65EB36 2B3CD612 40C1FCA8 7CC7D8A4 01FA5D9C C2DBC999
        B55354A4 F921FC42 19D334D4 F71CD68E B19220A1 D20D829D
        95FB8785 A30A0B59 562FB7E9 250CD095 0B80C397 01D71C9F
        78D4C735 40C4F606 26400F43 5D0BB59C 579E0BF8 7475620F
        0CFB6D3F 89F27C8D 0A9C2A40 BED5D71C 10ED6C99 9FBDB3B7


MacKey is
        3D4C2DF7 DCEDD76A 9A744D98 265C64BE 518214D7 CF0C80BE


Mtag is
        B5E336D3 51CF280C 9B6C3DBE 1A910D37 9BD0E642 053ED50E
        08850300 88B345FF D189F9D5 0D2F7B5F 32E24F23 E33B0B8D


KeyData is
        E264E3D0 BD3CD563 355ACD02 9CF8E011 9EC24B62 C58D4AA7
        5F0DE506 BBF3982D 05383F41 B31778FE 235B7897 1F6448C3
        12BDE4D4 B3DE57FA 404F4C01 ACD2F1E2 78C41DB5 1350B550
        BB1F3657 C5AF67A2 235528E4 07B38283 3D1CB7CC 02A61D62




EphemeralUnifiedCDH(B-409)
------------------------------------------------------------
deU is
                                                    006EF9F6
        34CCE619 5CBF086A 40C58EB4 EAD07416 BD901E5C 3705EC7F
        9231DB0C A2A6020A FBD992AB 6698B1A3 ABBEF462 A1ADBC84


QeU_x is
                                                    01FA5D9C
        C2DBC999 B55354A4 F921FC42 19D334D4 F71CD68E B19220A1
        D20D829D 95FB8785 A30A0B59 562FB7E9 250CD095 0B80C397


QeU_y is
                                                    01D71C9F
        78D4C735 40C4F606 26400F43 5D0BB59C 579E0BF8 7475620F
        0CFB6D3F 89F27C8D 0A9C2A40 BED5D71C 10ED6C99 9FBDB3B7
```

```
deV is
                                                        0027B021
        03600E10 CBAF0D99 A01A3C19 B56C2D05 2693A382 07677E5B
        1149CE1A 146AA137 D0C9524E 199D5CE3 432B05A2 131ECB50


QeV_x is
                                                        01D325B4
        1C395BF7 31500C87 1043A032 6F4CA12D 8B124FD6 C17A13B5
        246C220B DA903A84 8AE6682F FF4BF764 874E06D9 8FBABC29


QeV_y is
                                                        0116CD16
        69FBE8BD CC7A1DA6 D9D88055 EDDF361C DF245140 0B65D868
        1DCA400F 5332374B 4E65EB36 2B3CD612 40C1FCA8 7CC7D8A4




------------------------------------------------------------
no Key Confirmation
Z is
                                                        0006FAD8
        492E08DE 6B2F938B A5B6BA28 1E995EEC D540D788 6BD6EAA3
        7E6C1FC5 3EAA5B33 65DFEA24 35082CFC C68BF9E3 2A53E641


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        3108CD9C 1D3ED0F8 7D90B959 E7457E17 F4884A28 DE42AFB8
        983E52B3 00AF0957 BBC34586 88755488 17A3C9C1 390BB561
        AD6F389B B739F79A 64FA1F1A D6B7F69D F3F0927C 1D13EC24
        03CE4D30 4AF6E298 643C4123 78CE27B6 CFDB4626 6E3E7132


KeyData is
        3108CD9C 1D3ED0F8 7D90B959 E7457E17 F4884A28 DE42AFB8
        983E52B3 00AF0957 BBC34586 88755488 17A3C9C1 390BB561
        AD6F389B B739F79A 64FA1F1A D6B7F69D F3F0927C 1D13EC24
        03CE4D30 4AF6E298 643C4123 78CE27B6 CFDB4626 6E3E7132
```

OnePassUnifiedCDH(B-409)
---

dsU is

00F2A861
311B086F 575FC709 16F04E30 44FB4CA3 12C352FF 0C12ED4A
AB990E1B 8D929967 BD55C76D 03390257 5969437E 73A68381

QsU_x is

01EFFB75
A8476005 0D112FA8 05106512 2D9A24EF 28FDD510 91E94FD3
E868F036 5063DC0C CAF6D734 2CBEED5C F69C835B 681E6B43

QsU_y is

005A8E93
A6E264AC CB9862FB 3ECF72D1 97E509CC 850FAE8E 76D33FD2
8FD45E95 459D68E0 9C42097C 2750995B 19846B2D 02EA425F

dsV is

0047F7DF
0EB6F57C 05B83D7F 7AD60D30 F1134508 F305AD88 7CA2850A
9E2AE76D 366CD506 AA90E9DA 3D184122 31ED33A0 280A5792

QsV_x is

0138DF61
834D9C39 AA3B157B 263AB64C 570239BB 6DD4120B A8E3F13D
E3CE17C5 5B87A655 20577E88 9B9BB7E3 190E095E C551A53D

QsV_y is

007FF7B7
79B76892 2E13A3DF AABDF60F 056B6F6D 2F2EEEE8 C0CB50AE
F0816E5A 21EE4E6A FC6E75FD F532CEA6 EA4F99DF DAC6BF32

deU is

006EF9F6
34CCE619 5CBF086A 40C58EB4 EAD07416 BD901E5C 3705EC7F
9231DB0C A2A6020A FBD992AB 6698B1A3 ABBEF462 A1ADBC84

```
QeU_x is
                                                        01FA5D9C
        C2DBC999 B55354A4 F921FC42 19D334D4 F71CD68E B19220A1
        D20D829D 95FB8785 A30A0B59 562FB7E9 250CD095 0B80C397


QeU_y is
                                                        01D71C9F
        78D4C735 40C4F606 26400F43 5D0BB59C 579E0BF8 7475620F
        0CFB6D3F 89F27C8D 0A9C2A40 BED5D71C 10ED6C99 9FBDB3B7




------------------------------------------------------------
no Key Confirmation
Zs is
                                                        00494A68
        E6BF47C7 7402FF79 82950101 E92F2D78 C7A59A85 ACF56F11
        57F28B49 8DAB7392 C933B149 54D54F88 8355B87A 80B16E8D


Ze is
                                                        00EC676C
        987ACE51 FBDD065B 081A58D0 4386E1C0 96A1BD03 544B4EF1
        EF859D1C C8B3AD2C 84363AA4 90AA9317 FE915E4E F50FCBB1


Z is
                                                00EC676C 987ACE51
        FBDD065B 081A58D0 4386E1C0 96A1BD03 544B4EF1 EF859D1C
        C8B3AD2C 84363AA4 90AA9317 FE915E4E F50FCBB1 00494A68
        E6BF47C7 7402FF79 82950101 E92F2D78 C7A59A85 ACF56F11
        57F28B49 8DAB7392 C933B149 54D54F88 8355B87A 80B16E8D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        74BCE8AC 451C397A C0CAA2DC 7DC5FD2A 96540A48 FFBD10ED
        16D513C2 6F6E5628 C31E32B6 688F9BE9 262AEDBC A96C0370
        B1AC1ADC 32359937 1D6CD238 108C3566 F612B60C A1CDDAD8
        B0724E52 1954D226 BAC95503 89051545 BE2EFA7A 3E384F60
```

KeyData is
        74BCE8AC 451C397A C0CAA2DC 7DC5FD2A 96540A48 FFBD10ED
        16D513C2 6F6E5628 C31E32B6 688F9BE9 262AEDBC A96C0370
        B1AC1ADC 32359937 1D6CD238 108C3566 F612B60C A1CDDAD8
        B0724E52 1954D226 BAC95503 89051545 BE2EFA7A 3E384F60

Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                                                    0090F0B2
        F19590E2 3ADC6562 8A0BEA3C 2BD141EC E9F4F4E8 66AE175D
        FC3ABB5A F94005E6 D3C86B32 690298FA FCC0E3AA E4453ECF

Zs is
                                                    00494A68
        E6BF47C7 7402FF79 82950101 E92F2D78 C7A59A85 ACF56F11
        57F28B49 8DAB7392 C933B149 54D54F88 8355B87A 80B16E8D

Ze is
                                                    00EC676C
        987ACE51 FBDD065B 081A58D0 4386E1C0 96A1BD03 544B4EF1
        EF859D1C C8B3AD2C 84363AA4 90AA9317 FE915E4E F50FCBB1

Z is
                                            00EC676C 987ACE51
        FBDD065B 081A58D0 4386E1C0 96A1BD03 544B4EF1 EF859D1C
        C8B3AD2C 84363AA4 90AA9317 FE915E4E F50FCBB1 00494A68
        E6BF47C7 7402FF79 82950101 E92F2D78 C7A59A85 ACF56F11
        57F28B49 8DAB7392 C933B149 54D54F88 8355B87A 80B16E8D

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
        74BCE8AC 451C397A C0CAA2DC 7DC5FD2A 96540A48 FFBD10ED
        16D513C2 6F6E5628 C31E32B6 688F9BE9 262AEDBC A96C0370

```
        B1AC1ADC 32359937 1D6CD238 108C3566 F612B60C A1CDDAD8
        B0724E52 1954D226 BAC95503 89051545 BE2EFA7A 3E384F60
        C3E7A2C2 84287ABD 38B4FDD7 BEFEC681 EF2EAC58 A7CDE371


MacData is
                                                    4B435F31
        5F55414C 49434542 4F424259 01FA5D9C C2DBC999 B55354A4
        F921FC42 19D334D4 F71CD68E B19220A1 D20D829D 95FB8785
        A30A0B59 562FB7E9 250CD095 0B80C397 01D71C9F 78D4C735
        40C4F606 26400F43 5D0BB59C 579E0BF8 7475620F 0CFB6D3F
        89F27C8D 0A9C2A40 BED5D71C 10ED6C99 9FBDB3B7 0090F0B2
        F19590E2 3ADC6562 8A0BEA3C 2BD141EC E9F4F4E8 66AE175D
        FC3ABB5A F94005E6 D3C86B32 690298FA FCC0E3AA E4453ECF


MacKey is
        74BCE8AC 451C397A C0CAA2DC 7DC5FD2A 96540A48 FFBD10ED


Mtag is
        51DA2C52 28C72DC5 7F5B93F9 289A1EF3 4921EC9D 015798A4
        31F754C4 EEFB2ADF 4638AF8B E23904CD 5DB3D81D 4126B128


KeyData is
        16D513C2 6F6E5628 C31E32B6 688F9BE9 262AEDBC A96C0370
        B1AC1ADC 32359937 1D6CD238 108C3566 F612B60C A1CDDAD8
        B0724E52 1954D226 BAC95503 89051545 BE2EFA7A 3E384F60
        C3E7A2C2 84287ABD 38B4FDD7 BEFEC681 EF2EAC58 A7CDE371




-----------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
                                                    0090F0B2
        F19590E2 3ADC6562 8A0BEA3C 2BD141EC E9F4F4E8 66AE175D
        FC3ABB5A F94005E6 D3C86B32 690298FA FCC0E3AA E4453ECF


Zs is
                                                    00494A68
        E6BF47C7 7402FF79 82950101 E92F2D78 C7A59A85 ACF56F11
        57F28B49 8DAB7392 C933B149 54D54F88 8355B87A 80B16E8D
```

Ze is
                                                    00EC676C
        987ACE51 FBDD065B 081A58D0 4386E1C0 96A1BD03 544B4EF1
        EF859D1C C8B3AD2C 84363AA4 90AA9317 FE915E4E F50FCBB1

Z is
                                                00EC676C 987ACE51
        FBDD065B 081A58D0 4386E1C0 96A1BD03 544B4EF1 EF859D1C
        C8B3AD2C 84363AA4 90AA9317 FE915E4E F50FCBB1 00494A68
        E6BF47C7 7402FF79 82950101 E92F2D78 C7A59A85 ACF56F11
        57F28B49 8DAB7392 C933B149 54D54F88 8355B87A 80B16E8D

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
        74BCE8AC 451C397A C0CAA2DC 7DC5FD2A 96540A48 FFBD10ED
        16D513C2 6F6E5628 C31E32B6 688F9BE9 262AEDBC A96C0370
        B1AC1ADC 32359937 1D6CD238 108C3566 F612B60C A1CDDAD8
        B0724E52 1954D226 BAC95503 89051545 BE2EFA7A 3E384F60
        C3E7A2C2 84287ABD 38B4FDD7 BEFEC681 EF2EAC58 A7CDE371

MacData is
        4B435F31 5F56424F 42425941 4C494345 01FA5D9C C2DBC999
        B55354A4 F921FC42 19D334D4 F71CD68E B19220A1 D20D829D
        95FB8785 A30A0B59 562FB7E9 250CD095 0B80C397 01D71C9F
        78D4C735 40C4F606 26400F43 5D0BB59C 579E0BF8 7475620F
        0CFB6D3F 89F27C8D 0A9C2A40 BED5D71C 10ED6C99 9FBDB3B7

MacKey is
        74BCE8AC 451C397A C0CAA2DC 7DC5FD2A 96540A48 FFBD10ED

Mtag is
        AD6405A6 B072108D B00704EB F342E4C7 04F719E8 061AACEB
        20FC7C08 9E667B59 FEE61AE2 ABD227BA 661FA0A9 C7658D45

KeyData is

16D513C2 6F6E5628 C31E32B6 688F9BE9 262AEDBC A96C0370
B1AC1ADC 32359937 1D6CD238 108C3566 F612B60C A1CDDAD8
B0724E52 1954D226 BAC95503 89051545 BE2EFA7A 3E384F60
C3E7A2C2 84287ABD 38B4FDD7 BEFEC681 EF2EAC58 A7CDE371

Scheme Initiator, Key Confirmation Bilateral
NonceV is
0090F0B2
F19590E2 3ADC6562 8A0BEA3C 2BD141EC E9F4F4E8 66AE175D
FC3ABB5A F94005E6 D3C86B32 690298FA FCC0E3AA E4453ECF

Zs is
00494A68
E6BF47C7 7402FF79 82950101 E92F2D78 C7A59A85 ACF56F11
57F28B49 8DAB7392 C933B149 54D54F88 8355B87A 80B16E8D

Ze is
00EC676C
987ACE51 FBDD065B 081A58D0 4386E1C0 96A1BD03 544B4EF1
EF859D1C C8B3AD2C 84363AA4 90AA9317 FE915E4E F50FCBB1

Z is
00EC676C 987ACE51
FBDD065B 081A58D0 4386E1C0 96A1BD03 544B4EF1 EF859D1C
C8B3AD2C 84363AA4 90AA9317 FE915E4E F50FCBB1 00494A68
E6BF47C7 7402FF79 82950101 E92F2D78 C7A59A85 ACF56F11
57F28B49 8DAB7392 C933B149 54D54F88 8355B87A 80B16E8D

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
74BCE8AC 451C397A C0CAA2DC 7DC5FD2A 96540A48 FFBD10ED
16D513C2 6F6E5628 C31E32B6 688F9BE9 262AEDBC A96C0370
B1AC1ADC 32359937 1D6CD238 108C3566 F612B60C A1CDDAD8
B0724E52 1954D226 BAC95503 89051545 BE2EFA7A 3E384F60
C3E7A2C2 84287ABD 38B4FDD7 BEFEC681 EF2EAC58 A7CDE371

U2V

MacData is
                                                        4B435F32
        5F55414C 49434542 4F424259 01FA5D9C C2DBC999 B55354A4
        F921FC42 19D334D4 F71CD68E B19220A1 D20D829D 95FB8785
        A30A0B59 562FB7E9 250CD095 0B80C397 01D71C9F 78D4C735
        40C4F606 26400F43 5D0BB59C 579E0BF8 7475620F 0CFB6D3F
        89F27C8D 0A9C2A40 BED5D71C 10ED6C99 9FBDB3B7 0090F0B2
        F19590E2 3ADC6562 8A0BEA3C 2BD141EC E9F4F4E8 66AE175D
        FC3ABB5A F94005E6 D3C86B32 690298FA FCC0E3AA E4453ECF

MacKey is
        74BCE8AC 451C397A C0CAA2DC 7DC5FD2A 96540A48 FFBD10ED

Mtag is
        5E535986 9B28C41F E80E464C E2BB9DE7 83F08C4A EAA67E37
        6C8488ED 4DA40EE5 EB405610 B2854A9F 529C8311 6B4378A5

V2U

MacData is
                                                        4B435F32
        5F56424F 42425941 4C494345 0090F0B2 F19590E2 3ADC6562
        8A0BEA3C 2BD141EC E9F4F4E8 66AE175D FC3ABB5A F94005E6
        D3C86B32 690298FA FCC0E3AA E4453ECF 01FA5D9C C2DBC999
        B55354A4 F921FC42 19D334D4 F71CD68E B19220A1 D20D829D
        95FB8785 A30A0B59 562FB7E9 250CD095 0B80C397 01D71C9F
        78D4C735 40C4F606 26400F43 5D0BB59C 579E0BF8 7475620F
        0CFB6D3F 89F27C8D 0A9C2A40 BED5D71C 10ED6C99 9FBDB3B7

MacKey is
        74BCE8AC 451C397A C0CAA2DC 7DC5FD2A 96540A48 FFBD10ED

Mtag is
        476DAF2D 576FAC3E F42E3F5B F4171487 2007A290 F2E24D36
        B0AD2ADA 2EF3F2C2 C555FA48 E741AA93 AED3DD99 9398D964

KeyData is
        16D513C2 6F6E5628 C31E32B6 688F9BE9 262AEDBC A96C0370
        B1AC1ADC 32359937 1D6CD238 108C3566 F612B60C A1CDDAD8
        B0724E52 1954D226 BAC95503 89051545 BE2EFA7A 3E384F60
        C3E7A2C2 84287ABD 38B4FDD7 BEFEC681 EF2EAC58 A7CDE371

OnePassMQV(B-409)
----
dsU is
                                                    00F2A861
        311B086F 575FC709 16F04E30 44FB4CA3 12C352FF 0C12ED4A
        AB990E1B 8D929967 BD55C76D 03390257 5969437E 73A68381

QsU_x is
                                                    01EFFB75
        A8476005 0D112FA8 05106512 2D9A24EF 28FDD510 91E94FD3
        E868F036 5063DC0C CAF6D734 2CBEED5C F69C835B 681E6B43

QsU_y is
                                                    005A8E93
        A6E264AC CB9862FB 3ECF72D1 97E509CC 850FAE8E 76D33FD2
        8FD45E95 459D68E0 9C42097C 2750995B 19846B2D 02EA425F

dsV is
                                                    0047F7DF
        0EB6F57C 05B83D7F 7AD60D30 F1134508 F305AD88 7CA2850A
        9E2AE76D 366CD506 AA90E9DA 3D184122 31ED33A0 280A5792

QsV_x is
                                                    0138DF61
        834D9C39 AA3B157B 263AB64C 570239BB 6DD4120B A8E3F13D
        E3CE17C5 5B87A655 20577E88 9B9BB7E3 190E095E C551A53D

QsV_y is
                                                    007FF7B7
        79B76892 2E13A3DF AABDF60F 056B6F6D 2F2EEEE8 C0CB50AE
        F0816E5A 21EE4E6A FC6E75FD F532CEA6 EA4F99DF DAC6BF32

```
deU is
                                                        006EF9F6
        34CCE619 5CBF086A 40C58EB4 EAD07416 BD901E5C 3705EC7F
        9231DB0C A2A6020A FBD992AB 6698B1A3 ABBEF462 A1ADBC84


QeU_x is
                                                        01FA5D9C
        C2DBC999 B55354A4 F921FC42 19D334D4 F71CD68E B19220A1
        D20D829D 95FB8785 A30A0B59 562FB7E9 250CD095 0B80C397


QeU_y is
                                                        01D71C9F
        78D4C735 40C4F606 26400F43 5D0BB59C 579E0BF8 7475620F
        0CFB6D3F 89F27C8D 0A9C2A40 BED5D71C 10ED6C99 9FBDB3B7




------------------------------------------------------------
no Key Confirmation
Z is
                                                        00787B36
        7BF6CD7E 05B0A9E0 68C6C491 3009DDE6 DC3D7AE1 C48723CD
        6BEDE970 1040EB0E 2CEBD6E2 1F8DE022 7A6A82BB 47430801


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        C78FCD35 B2B4E00A 9B2EF589 E16CC53D ECEA26F1 83F80D81
        BE0E1AC9 853E8315 C3C4DF21 5DC984AF 03EF02D9 0E9C5A5C
        0F0BB0FF 9C2195D1 B248113B E62165DD 3E81AC50 4BF4AA41
        5361AF36 532D4D7F BBA6434D BC4A937D DB09BC55 C8404246


KeyData is
        C78FCD35 B2B4E00A 9B2EF589 E16CC53D ECEA26F1 83F80D81
        BE0E1AC9 853E8315 C3C4DF21 5DC984AF 03EF02D9 0E9C5A5C
        0F0BB0FF 9C2195D1 B248113B E62165DD 3E81AC50 4BF4AA41
        5361AF36 532D4D7F BBA6434D BC4A937D DB09BC55 C8404246
```

```
------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                                                        0090F0B2
        F19590E2 3ADC6562 8A0BEA3C 2BD141EC E9F4F4E8 66AE175D
        FC3ABB5A F94005E6 D3C86B32 690298FA FCC0E3AA E4453ECF


Z is
                                                        00787B36
        7BF6CD7E 05B0A9E0 68C6C491 3009DDE6 DC3D7AE1 C48723CD
        6BEDE970 1040EB0E 2CEBD6E2 1F8DE022 7A6A82BB 47430801


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        C78FCD35 B2B4E00A 9B2EF589 E16CC53D ECEA26F1 83F80D81
        BE0E1AC9 853E8315 C3C4DF21 5DC984AF 03EF02D9 0E9C5A5C
        0F0BB0FF 9C2195D1 B248113B E62165DD 3E81AC50 4BF4AA41
        5361AF36 532D4D7F BBA6434D BC4A937D DB09BC55 C8404246
        DF8B9144 FD2F59D4 24D7E5C0 AB765CD9 94641440 57A0911C


MacData is
                                                        4B435F31
        5F55414C 49434542 4F424259 01FA5D9C C2DBC999 B55354A4
        F921FC42 19D334D4 F71CD68E B19220A1 D20D829D 95FB8785
        A30A0B59 562FB7E9 250CD095 0B80C397 01D71C9F 78D4C735
        40C4F606 26400F43 5D0BB59C 579E0BF8 7475620F 0CFB6D3F
        89F27C8D 0A9C2A40 BED5D71C 10ED6C99 9FBDB3B7 0090F0B2
        F19590E2 3ADC6562 8A0BEA3C 2BD141EC E9F4F4E8 66AE175D
        FC3ABB5A F94005E6 D3C86B32 690298FA FCC0E3AA E4453ECF


MacKey is
        C78FCD35 B2B4E00A 9B2EF589 E16CC53D ECEA26F1 83F80D81


Mtag is
        CB3AC6CC F882AFD4 702929DB 23C9134C DA5BEBF6 543ACFE5
```

AFBE57B8 08DFF86B 332BA597 10AEA9B9 B850EC97 E3003D1A

KeyData is
BE0E1AC9 853E8315 C3C4DF21 5DC984AF 03EF02D9 0E9C5A5C
0F0BB0FF 9C2195D1 B248113B E62165DD 3E81AC50 4BF4AA41
5361AF36 532D4D7F BBA6434D BC4A937D DB09BC55 C8404246
DF8B9144 FD2F59D4 24D7E5C0 AB765CD9 94641440 57A0911C

Scheme Responder, Key Confirmation Provider: V to U
NonceU is
0090F0B2
F19590E2 3ADC6562 8A0BEA3C 2BD141EC E9F4F4E8 66AE175D
FC3ABB5A F94005E6 D3C86B32 690298FA FCC0E3AA E4453ECF

Z is
00787B36
7BF6CD7E 05B0A9E0 68C6C491 3009DDE6 DC3D7AE1 C48723CD
6BEDE970 1040EB0E 2CEBD6E2 1F8DE022 7A6A82BB 47430801

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
C78FCD35 B2B4E00A 9B2EF589 E16CC53D ECEA26F1 83F80D81
BE0E1AC9 853E8315 C3C4DF21 5DC984AF 03EF02D9 0E9C5A5C
0F0BB0FF 9C2195D1 B248113B E62165DD 3E81AC50 4BF4AA41
5361AF36 532D4D7F BBA6434D BC4A937D DB09BC55 C8404246
DF8B9144 FD2F59D4 24D7E5C0 AB765CD9 94641440 57A0911C

MacData is
4B435F31 5F56424F 42425941 4C494345 01FA5D9C C2DBC999
B55354A4 F921FC42 19D334D4 F71CD68E B19220A1 D20D829D
95FB8785 A30A0B59 562FB7E9 250CD095 0B80C397 01D71C9F
78D4C735 40C4F606 26400F43 5D0BB59C 579E0BF8 7475620F
0CFB6D3F 89F27C8D 0A9C2A40 BED5D71C 10ED6C99 9FBDB3B7

```
MacKey is
        C78FCD35 B2B4E00A 9B2EF589 E16CC53D ECEA26F1 83F80D81


Mtag is
        1B120547 69AC2721 AD513964 C4C42E83 A05130B2 C0634575
        5DE322F8 D2DBFCF9 061731DE B7F974BD C38A0254 66D1DD15


KeyData is
        BE0E1AC9 853E8315 C3C4DF21 5DC984AF 03EF02D9 0E9C5A5C
        0F0BB0FF 9C2195D1 B248113B E62165DD 3E81AC50 4BF4AA41
        5361AF36 532D4D7F BBA6434D BC4A937D DB09BC55 C8404246
        DF8B9144 FD2F59D4 24D7E5C0 AB765CD9 94641440 57A0911C




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
                                                        0090F0B2
        F19590E2 3ADC6562 8A0BEA3C 2BD141EC E9F4F4E8 66AE175D
        FC3ABB5A F94005E6 D3C86B32 690298FA FCC0E3AA E4453ECF


Z is
                                                        00787B36
        7BF6CD7E 05B0A9E0 68C6C491 3009DDE6 DC3D7AE1 C48723CD
        6BEDE970 1040EB0E 2CEBD6E2 1F8DE022 7A6A82BB 47430801


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        C78FCD35 B2B4E00A 9B2EF589 E16CC53D ECEA26F1 83F80D81
        BE0E1AC9 853E8315 C3C4DF21 5DC984AF 03EF02D9 0E9C5A5C
        0F0BB0FF 9C2195D1 B248113B E62165DD 3E81AC50 4BF4AA41
        5361AF36 532D4D7F BBA6434D BC4A937D DB09BC55 C8404246
        DF8B9144 FD2F59D4 24D7E5C0 AB765CD9 94641440 57A0911C


U2V
----------------
```

```
MacData is
                                                        4B435F32
        5F55414C 49434542 4F424259 01FA5D9C C2DBC999 B55354A4
        F921FC42 19D334D4 F71CD68E B19220A1 D20D829D 95FB8785
        A30A0B59 562FB7E9 250CD095 0B80C397 01D71C9F 78D4C735
        40C4F606 26400F43 5D0BB59C 579E0BF8 7475620F 0CFB6D3F
        89F27C8D 0A9C2A40 BED5D71C 10ED6C99 9FBDB3B7 0090F0B2
        F19590E2 3ADC6562 8A0BEA3C 2BD141EC E9F4F4E8 66AE175D
        FC3ABB5A F94005E6 D3C86B32 690298FA FCC0E3AA E4453ECF


MacKey is
        C78FCD35 B2B4E00A 9B2EF589 E16CC53D ECEA26F1 83F80D81


Mtag is
        92015BE0 048DADFA 789BB7FF 42F1899C E8FBF64D 25B1B914
        01EA21D5 D3E4A4E0 FAE0C189 6C60A039 ACE30CCA 362817FF


V2U
----------------
MacData is
                                                        4B435F32
        5F56424F 42425941 4C494345 0090F0B2 F19590E2 3ADC6562
        8A0BEA3C 2BD141EC E9F4F4E8 66AE175D FC3ABB5A F94005E6
        D3C86B32 690298FA FCC0E3AA E4453ECF 01FA5D9C C2DBC999
        B55354A4 F921FC42 19D334D4 F71CD68E B19220A1 D20D829D
        95FB8785 A30A0B59 562FB7E9 250CD095 0B80C397 01D71C9F
        78D4C735 40C4F606 26400F43 5D0BB59C 579E0BF8 7475620F
        0CFB6D3F 89F27C8D 0A9C2A40 BED5D71C 10ED6C99 9FBDB3B7


MacKey is
        C78FCD35 B2B4E00A 9B2EF589 E16CC53D ECEA26F1 83F80D81


Mtag is
        5F4161DD 885F3F69 151EEAB6 DFC3B868 71040AD3 AFC2B854
        4414FC7E 1BCA50A0 B13999E8 E53F9E5F D18D4663 FFFBA0B4


KeyData is
        BE0E1AC9 853E8315 C3C4DF21 5DC984AF 03EF02D9 0E9C5A5C
        0F0BB0FF 9C2195D1 B248113B E62165DD 3E81AC50 4BF4AA41
        5361AF36 532D4D7F BBA6434D BC4A937D DB09BC55 C8404246
```

```
        DF8B9144 FD2F59D4 24D7E5C0 AB765CD9 94641440 57A0911C



OnePassDiffieHellmanCDH(B-409)
------------------------------------------------------------
dsV is
                                                    0047F7DF
        0EB6F57C 05B83D7F 7AD60D30 F1134508 F305AD88 7CA2850A
        9E2AE76D 366CD506 AA90E9DA 3D184122 31ED33A0 280A5792


QsV_x is
                                                    0138DF61
        834D9C39 AA3B157B 263AB64C 570239BB 6DD4120B A8E3F13D
        E3CE17C5 5B87A655 20577E88 9B9BB7E3 190E095E C551A53D


QsV_y is
                                                    007FF7B7
        79B76892 2E13A3DF AABDF60F 056B6F6D 2F2EEEE8 C0CB50AE
        F0816E5A 21EE4E6A FC6E75FD F532CEA6 EA4F99DF DAC6BF32


deU is
                                                    006EF9F6
        34CCE619 5CBF086A 40C58EB4 EAD07416 BD901E5C 3705EC7F
        9231DB0C A2A6020A FBD992AB 6698B1A3 ABBEF462 A1ADBC84


QeU_x is
                                                    01FA5D9C
        C2DBC999 B55354A4 F921FC42 19D334D4 F71CD68E B19220A1
        D20D829D 95FB8785 A30A0B59 562FB7E9 250CD095 0B80C397


QeU_y is
                                                    01D71C9F
        78D4C735 40C4F606 26400F43 5D0BB59C 579E0BF8 7475620F
        0CFB6D3F 89F27C8D 0A9C2A40 BED5D71C 10ED6C99 9FBDB3B7



------------------------------------------------------------
```

no Key Confirmation
Z is
                                                        00EC676C
        987ACE51 FBDD065B 081A58D0 4386E1C0 96A1BD03 544B4EF1
        EF859D1C C8B3AD2C 84363AA4 90AA9317 FE915E4E F50FCBB1

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
        C0437075 1E1AFC8D CB81E205 009385AB B6ED75AC 4F88ADCC
        6912F289 47C1CF2B 7199D844 1919B16C 13FBD094 FCBECD62
        4572A571 F3B0DB1E D6BAED41 20377020 4009A00D 310D8EB3
        926CBC74 A9AFEA04 32DC9F78 28792EF9 015C4448 28570635

KeyData is
        C0437075 1E1AFC8D CB81E205 009385AB B6ED75AC 4F88ADCC
        6912F289 47C1CF2B 7199D844 1919B16C 13FBD094 FCBECD62
        4572A571 F3B0DB1E D6BAED41 20377020 4009A00D 310D8EB3
        926CBC74 A9AFEA04 32DC9F78 28792EF9 015C4448 28570635

Scheme Responder, Key Confirmation Provider: V to U
Z is
                                                        00EC676C
        987ACE51 FBDD065B 081A58D0 4386E1C0 96A1BD03 544B4EF1
        EF859D1C C8B3AD2C 84363AA4 90AA9317 FE915E4E F50FCBB1

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
        C0437075 1E1AFC8D CB81E205 009385AB B6ED75AC 4F88ADCC
        6912F289 47C1CF2B 7199D844 1919B16C 13FBD094 FCBECD62
        4572A571 F3B0DB1E D6BAED41 20377020 4009A00D 310D8EB3
        926CBC74 A9AFEA04 32DC9F78 28792EF9 015C4448 28570635
        D184EB13 6CE19927 FF8725C0 CD34D483 098B36D4 6A212C5A

MacData is
	4B435F31 5F56424F 42425941 4C494345 01FA5D9C C2DBC999
	B55354A4 F921FC42 19D334D4 F71CD68E B19220A1 D20D829D
	95FB8785 A30A0B59 562FB7E9 250CD095 0B80C397 01D71C9F
	78D4C735 40C4F606 26400F43 5D0BB59C 579E0BF8 7475620F
	0CFB6D3F 89F27C8D 0A9C2A40 BED5D71C 10ED6C99 9FBDB3B7

MacKey is
	C0437075 1E1AFC8D CB81E205 009385AB B6ED75AC 4F88ADCC

Mtag is
	0B2F1A79 B9405D4C C7E07549 E0B4E98D 7165D64E FA5841CE
	279911EA E2344E53 B5AD893B DE0225E4 08BF8D16 6E0877A5

KeyData is
	6912F289 47C1CF2B 7199D844 1919B16C 13FBD094 FCBECD62
	4572A571 F3B0DB1E D6BAED41 20377020 4009A00D 310D8EB3
	926CBC74 A9AFEA04 32DC9F78 28792EF9 015C4448 28570635
	D184EB13 6CE19927 FF8725C0 CD34D483 098B36D4 6A212C5A

StaticUnifiedCDH(B-409)
---
dsU is
	00F2A861
	311BF60B A6287195 DB1A0328 4F17DC1B D33E5C21 06A4502B
	5C572CBE D58314B5 A7965DB1 BC63A482 8E683964 0199651F

QsU_x is
	00567959
	EF7F70D7 A0BDDBB7 381DB57B E38B5DC6 5A07133A C278D3AA
	E783FBB0 772C87B5 184168FE 85135A51 C281990E 35E653A7

QsU_y is
	00BC2307
	F413E705 72D88A24 97248D5C 8152EDA0 9565A79A D13EDC53
	8B32D425 2105CADC F525EBE3 E4ECA627 3B8AB281 21B04E40

```
dsV is
                                                        0047F7DF
        0EB70944 4964C14C 0BB787A6 FCD0BED5 0B6BC36F F0BAAAE8
        6E3D120B 62639242 A16B8DEF 865BBEDD 3E8E73DF D310C7BE


QsV_x is
                                                        001FDFF0
        A41D7958 A59082B1 78C598FE 527BF807 541703A1 2E7DC07B
        DB09846D 74B3CD7B 337C30B7 08BF02A4 8A4BA13B E6C344A7


QsV_y is
                                                        002CD0AE
        D6FD8642 BE47A011 E69F77F9 FBB50C1A 085E7B08 94FB3140
        F0B8BF1D 38D30FC5 5CE37BC0 8FC6649D 8D0A28DE 58147190




------------------------------------------------------------
no Key Confirmation
NonceU is
                                                        0090F0B2
        F19590E2 3ADC6562 8A0BEA3C 2BD141EC E9F4F4E8 66AE175D
        FC3ABB5A F94005E6 D3C86B32 690298FA FCC0E3AA E4453ECF


Z is
                                                        0119308D
        CE528008 B131827B B2D193B6 AB3498B5 2717BBF9 06065E93
        A4B68F59 6E1B0715 C965EF3F 2E596256 A2E119FC F135A5CD


OtherInfo is
                                                    1234 56789ABC
        DEF0414C 49434531 32339901 0090F0B2 F19590E2 3ADC6562
        8A0BEA3C 2BD141EC E9F4F4E8 66AE175D FC3ABB5A F94005E6
        D3C86B32 690298FA FCC0E3AA E4453ECF 424F4242 59343536


DerivedKeyMaterial is
        9654F991 79760DF6 53ACB4C3 1F1ACF18 A342B495 0B5C8C46
        91BA4D8E 3AF02844 4EBFEB79 320498E6 341CA1E4 BD78E077
        5E806E3C DBC89A5B 3031A359 21B0DAFD FE1E6052 0C1CEAEC
```

```
        FD6AE292 8161A63C AF0FE338 CB4D65E6 55755734 6C654C2B


KeyData is
        9654F991 79760DF6 53ACB4C3 1F1ACF18 A342B495 0B5C8C46
        91BA4D8E 3AF02844 4EBFEB79 320498E6 341CA1E4 BD78E077
        5E806E3C DBC89A5B 3031A359 21B0DAFD FE1E6052 0C1CEAEC
        FD6AE292 8161A63C AF0FE338 CB4D65E6 55755734 6C654C2B




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceU is
                                                    0090F0B2
        F19590E2 3ADC6562 8A0BEA3C 2BD141EC E9F4F4E8 66AE175D
        FC3ABB5A F94005E6 D3C86B32 690298FA FCC0E3AA E4453ECF


NonceV is
                                                    00AB5F06
        5A4474AE 5CD414F7 5FADD645 10A87D36 F7A93F14 7D087EB4
        47EF8B02 19855693 8CDE7E36 AA15D4A4 B549E845 61AC8D24


Z is
                                                    0119308D
        CE528008 B131827B B2D193B6 AB3498B5 2717BBF9 06065E93
        A4B68F59 6E1B0715 C965EF3F 2E596256 A2E119FC F135A5CD


OtherInfo is
                                                1234 56789ABC
        DEF0414C 49434531 32339901 0090F0B2 F19590E2 3ADC6562
        8A0BEA3C 2BD141EC E9F4F4E8 66AE175D FC3ABB5A F94005E6
        D3C86B32 690298FA FCC0E3AA E4453ECF 424F4242 59343536


DerivedKeyMaterial is
        9654F991 79760DF6 53ACB4C3 1F1ACF18 A342B495 0B5C8C46
        91BA4D8E 3AF02844 4EBFEB79 320498E6 341CA1E4 BD78E077
        5E806E3C DBC89A5B 3031A359 21B0DAFD FE1E6052 0C1CEAEC
        FD6AE292 8161A63C AF0FE338 CB4D65E6 55755734 6C654C2B
        63BABC42 E4314E91 2B26932D CBCCA920 30238718 C66D73E0
```

MacData is
4B435F31 5F55414C 49434542 4F424259 0090F0B2 F19590E2
3ADC6562 8A0BEA3C 2BD141EC E9F4F4E8 66AE175D FC3ABB5A
F94005E6 D3C86B32 690298FA FCC0E3AA E4453ECF 00AB5F06
5A4474AE 5CD414F7 5FADD645 10A87D36 F7A93F14 7D087EB4
47EF8B02 19855693 8CDE7E36 AA15D4A4 B549E845 61AC8D24

MacKey is
9654F991 79760DF6 53ACB4C3 1F1ACF18 A342B495 0B5C8C46

Mtag is
E097513D C8B108C9 FAE67003 4DD2C43F 246C4727 6F10EE4D
911522AB B54B00EE C4E7E77C 3D20576E 82A51A4F 5B93BC67

KeyData is
91BA4D8E 3AF02844 4EBFEB79 320498E6 341CA1E4 BD78E077
5E806E3C DBC89A5B 3031A359 21B0DAFD FE1E6052 0C1CEAEC
FD6AE292 8161A63C AF0FE338 CB4D65E6 55755734 6C654C2B
63BABC42 E4314E91 2B26932D CBCCA920 30238718 C66D73E0

Scheme Responder, Key Confirmation Provider: V to U
NonceV is
00AB5F06
5A4474AE 5CD414F7 5FADD645 10A87D36 F7A93F14 7D087EB4
47EF8B02 19855693 8CDE7E36 AA15D4A4 B549E845 61AC8D24

NonceU is
0090F0B2
F19590E2 3ADC6562 8A0BEA3C 2BD141EC E9F4F4E8 66AE175D
FC3ABB5A F94005E6 D3C86B32 690298FA FCC0E3AA E4453ECF

Z is
0119308D
CE528008 B131827B B2D193B6 AB3498B5 2717BBF9 06065E93
A4B68F59 6E1B0715 C965EF3F 2E596256 A2E119FC F135A5CD

```
OtherInfo is
                                                    1234 56789ABC
        DEF0414C 49434531 32339901 0090F0B2 F19590E2 3ADC6562
        8A0BEA3C 2BD141EC E9F4F4E8 66AE175D FC3ABB5A F94005E6
        D3C86B32 690298FA FCC0E3AA E4453ECF 424F4242 59343536


DerivedKeyMaterial is
        9654F991 79760DF6 53ACB4C3 1F1ACF18 A342B495 0B5C8C46
        91BA4D8E 3AF02844 4EBFEB79 320498E6 341CA1E4 BD78E077
        5E806E3C DBC89A5B 3031A359 21B0DAFD FE1E6052 0C1CEAEC
        FD6AE292 8161A63C AF0FE338 CB4D65E6 55755734 6C654C2B
        63BABC42 E4314E91 2B26932D CBCCA920 30238718 C66D73E0


MacData is
                 4B435F31 5F56424F 42425941 4C494345 0090F0B2
        F19590E2 3ADC6562 8A0BEA3C 2BD141EC E9F4F4E8 66AE175D
        FC3ABB5A F94005E6 D3C86B32 690298FA FCC0E3AA E4453ECF


MacKey is
        9654F991 79760DF6 53ACB4C3 1F1ACF18 A342B495 0B5C8C46


Mtag is
        ACB78880 7F1795BE 028888E5 6705A8DC 38FD87BE 9077C8CE
        AA43A51B F25630C8 3617F756 85C5E4DA 71EF222F 97CED871


KeyData is
        91BA4D8E 3AF02844 4EBFEB79 320498E6 341CA1E4 BD78E077
        5E806E3C DBC89A5B 3031A359 21B0DAFD FE1E6052 0C1CEAEC
        FD6AE292 8161A63C AF0FE338 CB4D65E6 55755734 6C654C2B
        63BABC42 E4314E91 2B26932D CBCCA920 30238718 C66D73E0




-------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
NonceU is
                                                        0090F0B2
        F19590E2 3ADC6562 8A0BEA3C 2BD141EC E9F4F4E8 66AE175D
```

```
        FC3ABB5A F94005E6 D3C86B32 690298FA FCC0E3AA E4453ECF


NonceV is
                                                          00AB5F06
        5A4474AE 5CD414F7 5FADD645 10A87D36 F7A93F14 7D087EB4
        47EF8B02 19855693 8CDE7E36 AA15D4A4 B549E845 61AC8D24


Z is
                                                          0119308D
        CE528008 B131827B B2D193B6 AB3498B5 2717BBF9 06065E93
        A4B68F59 6E1B0715 C965EF3F 2E596256 A2E119FC F135A5CD


OtherInfo is
                                                  1234 56789ABC
        DEF0414C 49434531 32339901 0090F0B2 F19590E2 3ADC6562
        8A0BEA3C 2BD141EC E9F4F4E8 66AE175D FC3ABB5A F94005E6
        D3C86B32 690298FA FCC0E3AA E4453ECF 424F4242 59343536


DerivedKeyMaterial is
        9654F991 79760DF6 53ACB4C3 1F1ACF18 A342B495 0B5C8C46
        91BA4D8E 3AF02844 4EBFEB79 320498E6 341CA1E4 BD78E077
        5E806E3C DBC89A5B 3031A359 21B0DAFD FE1E6052 0C1CEAEC
        FD6AE292 8161A63C AF0FE338 CB4D65E6 55755734 6C654C2B
        63BABC42 E4314E91 2B26932D CBCCA920 30238718 C66D73E0


U2V
----------------
MacData is
        4B435F32 5F55414C 49434542 4F424259 0090F0B2 F19590E2
        3ADC6562 8A0BEA3C 2BD141EC E9F4F4E8 66AE175D FC3ABB5A
        F94005E6 D3C86B32 690298FA FCC0E3AA E4453ECF 00AB5F06
        5A4474AE 5CD414F7 5FADD645 10A87D36 F7A93F14 7D087EB4
        47EF8B02 19855693 8CDE7E36 AA15D4A4 B549E845 61AC8D24


MacKey is
        9654F991 79760DF6 53ACB4C3 1F1ACF18 A342B495 0B5C8C46


Mtag is
        78976A76 B56A7EC5 3FBCF791 DDC2CA94 A287FF73 2F564273
```

```
        10C6D674 555CC838 68174036 5EB7F27D 92FB110C 20DDCC39


V2U
----------------
MacData is
        4B435F32 5F56424F 42425941 4C494345 00AB5F06 5A4474AE
        5CD414F7 5FADD645 10A87D36 F7A93F14 7D087EB4 47EF8B02
        19855693 8CDE7E36 AA15D4A4 B549E845 61AC8D24 0090F0B2
        F19590E2 3ADC6562 8A0BEA3C 2BD141EC E9F4F4E8 66AE175D
        FC3ABB5A F94005E6 D3C86B32 690298FA FCC0E3AA E4453ECF


MacKey is
        9654F991 79760DF6 53ACB4C3 1F1ACF18 A342B495 0B5C8C46


Mtag is
        BB8C6600 E76CE0D8 09CC8CAF 2AD3F213 EA660EA7 2AC5BD7F
        6E093D13 EC252D01 0ED991C8 B9D8D724 24834F05 9A042481


KeyData is
        91BA4D8E 3AF02844 4EBFEB79 320498E6 341CA1E4 BD78E077
        5E806E3C DBC89A5B 3031A359 21B0DAFD FE1E6052 0C1CEAEC
        FD6AE292 8161A63C AF0FE338 CB4D65E6 55755734 6C654C2B
        63BABC42 E4314E91 2B26932D CBCCA920 30238718 C66D73E0
```

FullUnifiedCDH(K-571)
---
dsU is
	009B592D 32F99420 05A38021 D26E7AA6 ED3E78BB DFF2A861
	311B89C9 9DF67762 8EE47F3D 71AE14C6 6EDF0B6C 474E6AA6
	92A4B5BF 3D0814BB 28F38344 D445A44E 5E5FEFBC 3C00978C

QsU_x is
	04F6BD3B 3800DEAF 6D729E0C 29320D34 9E0EFDB5 D74352FD
	DD7EBA85 0BCB04A9 D699EEEB F4204910 7FB65ED4 60CD36B8
	376E0946 56C72747 1BC9982C D5F6E4A8 BDF941DC 1194915B

QsU_y is
	02FD71C0 43003170 0BADD2FC 922C037D 1EABB673 481FE607
	93F1D296 BD59A52B 9A4358BE 99D858DB BECE5240 4358FA17
	9F18D497 E41C3EC4 59D78F2A 2C6F0EDA CC353AD8 59667EAB

dsV is
	01823854 AF10876C 19AEE8EC 6691AD9E 7E294860 5347F7DF
	0EB770FE EB2E71B9 8FAB326F FAEDFEE6 7093A304 8B79CA07
	C7A718DD 32DE5305 48D0FD9B 553AFC00 0E927766 61F71FBB

QsV_x is
	04C74E10 D370016A 080BEDD0 E852F986 EFC63CAC 08BF055C
	795CD634 DF8BEB7A 4411AB19 358E58AC 8000F22F 9528F4E1
	CBF128B6 B5871363 4D62415E BFCD5A5A 94653F8D FDF0703B

QsV_y is
	06E73204 610FA3AC B35DD890 F03D2E5C 9BFA20DD 29DA26B6
	4B13DEC6 399061A2 DB2BBB0B 6CCF848C 6567B5FA 220AB1B8
	2A70DF20 F2B4105B DA8520C2 02BF828A 56A67DDC B9E79B24

deU is
	013AC597 40DDBC84 E4803312 4D269467 71CC4872 706EF9F6
	34CE0E8A F1A227E8 E14A088E 9B274ADD 07249E3B 8FC69719
	10EDE19F 15F9CF94 6BF59829 1F372BD0 7CE0824B 40E5B486

```
QeU_x is
        0669AE9D 0C657ED8 5B6174DD FC33F02E 2A28B422 5A0BE50B
        DB8303E1 CFCEFFCC F113D6FA 07EEA236 E0E72BDE F678D424
        28CC0379 85DE19D4 E3BAF9A7 0B793CCD 0BC8E2EF E1AF5993


QeU_y is
        00D54789 9C67ED17 B5F8997E 0D119729 2D06062A 8E7E7459
        CE620B0A C3F633BD 4A8AF428 59A1B0F9 53193CA3 062D310D
        9620B72C CD1B0A68 B34E9DA0 AD18BA34 48140686 8A2A57F5


deV is
        0035076B C0FAE543 F8E32E41 3BD442A5 4EF489B8 9927B021
        0360F83F 8703C448 C72F4550 D6460FDD 1E576438 A072A2B1
        CD4477B6 F0D61E5F 6A9D281C 9A4BBB5F 14E13C1C 7C0500CD


QeV_x is
        0121E5C2 A9941CE7 4E7C7F6C 19247594 D9A29A06 FEE2ED16
        6947EBF2 090985BC 87BB3E0F B787B504 F125E780 143B7C7C
        110D3493 5BBBC05A D1CA0083 4F6FF877 40C15AA8 D097D03C


QeV_y is
        0426B4CC D1078B01 F93F9138 E2A6382D 28431357 64A6583E
        E5E2E53F 3DA6A97F 7C871BD0 AB5F3E8A EE7C11F2 398D8CC5
        91914622 D590C32A 64D2D536 AC342D10 8455F5DF FAD02D66




------------------------------------------------------------
no Key Confirmation
Zs is
        04E6EA7E EB79EE4B EFFDF2E6 E264A1E9 E4C309E7 5C5FA4C4
        517BFEEE 7D64F383 227A1FE2 75F10B0C D182638E 5AD75CD8
        4A7331D0 2AD199BE ECDC6756 EC094CE6 476B78C9 3AC8C02D


Ze is
        0534AAF3 25606A84 324A0E34 CFF02963 D125470F 92BA808D
        CEA30098 A4A8FD27 AFB134CE 22919C3E 02C5D19E 4676C5F2
        929A23B2 4B016F08 C99E7240 3FB59AD6 82D9B9EA A0D449A8
```

```
Z is
        0534AAF3 25606A84 324A0E34 CFF02963 D125470F 92BA808D
        CEA30098 A4A8FD27 AFB134CE 22919C3E 02C5D19E 4676C5F2
        929A23B2 4B016F08 C99E7240 3FB59AD6 82D9B9EA A0D449A8
        04E6EA7E EB79EE4B EFFDF2E6 E264A1E9 E4C309E7 5C5FA4C4
        517BFEEE 7D64F383 227A1FE2 75F10B0C D182638E 5AD75CD8
        4A7331D0 2AD199BE ECDC6756 EC094CE6 476B78C9 3AC8C02D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                            F4F990F3 3337F508
        E32EF04B B4FC6343 E66A81C1 DE1EBC2D A73E6C2F C66FC0F4
        EA78B1EA E1F8FEB9 337FA71D 404B30E7 4B064E66 2F12B477
        DC88A267 74379248 84874659 A63374D6 25BA8922 0758992D
        DB88CCD1 A6E03FD9 78B4C48A 361C4FD6 D39C0C9D DCDFBFCC
        E13B9DDD 8E0AE94E ECC7E6EE 81C09AF2 BFD22BC4 89171818


KeyData is
                                            F4F990F3 3337F508
        E32EF04B B4FC6343 E66A81C1 DE1EBC2D A73E6C2F C66FC0F4
        EA78B1EA E1F8FEB9 337FA71D 404B30E7 4B064E66 2F12B477
        DC88A267 74379248 84874659 A63374D6 25BA8922 0758992D
        DB88CCD1 A6E03FD9 78B4C48A 361C4FD6 D39C0C9D DCDFBFCC
        E13B9DDD 8E0AE94E ECC7E6EE 81C09AF2 BFD22BC4 89171818




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Zs is
        04E6EA7E EB79EE4B EFFDF2E6 E264A1E9 E4C309E7 5C5FA4C4
        517BFEEE 7D64F383 227A1FE2 75F10B0C D182638E 5AD75CD8
        4A7331D0 2AD199BE ECDC6756 EC094CE6 476B78C9 3AC8C02D


Ze is
        0534AAF3 25606A84 324A0E34 CFF02963 D125470F 92BA808D
        CEA30098 A4A8FD27 AFB134CE 22919C3E 02C5D19E 4676C5F2
        929A23B2 4B016F08 C99E7240 3FB59AD6 82D9B9EA A0D449A8
```

Z is
        0534AAF3 25606A84 324A0E34 CFF02963 D125470F 92BA808D
        CEA30098 A4A8FD27 AFB134CE 22919C3E 02C5D19E 4676C5F2
        929A23B2 4B016F08 C99E7240 3FB59AD6 82D9B9EA A0D449A8
        04E6EA7E EB79EE4B EFFDF2E6 E264A1E9 E4C309E7 5C5FA4C4
        517BFEEE 7D64F383 227A1FE2 75F10B0C D182638E 5AD75CD8
        4A7331D0 2AD199BE ECDC6756 EC094CE6 476B78C9 3AC8C02D

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                         F4F990F3 3337F508 E32EF04B B4FC6343
        E66A81C1 DE1EBC2D A73E6C2F C66FC0F4 EA78B1EA E1F8FEB9
        337FA71D 404B30E7 4B064E66 2F12B477 DC88A267 74379248
        84874659 A63374D6 25BA8922 0758992D DB88CCD1 A6E03FD9
        78B4C48A 361C4FD6 D39C0C9D DCDFBFCC E13B9DDD 8E0AE94E
        ECC7E6EE 81C09AF2 BFD22BC4 89171818 997C54F2 53EC81C6
        111AE8E5 70556882 76D23A42 EBC09714 98EE0850 89DC789D

MacData is
                         4B435F31 5F55414C 49434542 4F424259
        0669AE9D 0C657ED8 5B6174DD FC33F02E 2A28B422 5A0BE50B
        DB8303E1 CFCEFFCC F113D6FA 07EEA236 E0E72BDE F678D424
        28CC0379 85DE19D4 E3BAF9A7 0B793CCD 0BC8E2EF E1AF5993
        00D54789 9C67ED17 B5F8997E 0D119729 2D06062A 8E7E7459
        CE620B0A C3F633BD 4A8AF428 59A1B0F9 53193CA3 062D310D
        9620B72C CD1B0A68 B34E9DA0 AD18BA34 48140686 8A2A57F5
        0121E5C2 A9941CE7 4E7C7F6C 19247594 D9A29A06 FEE2ED16
        6947EBF2 090985BC 87BB3E0F B787B504 F125E780 143B7C7C
        110D3493 5BBBC05A D1CA0083 4F6FF877 40C15AA8 D097D03C
        0426B4CC D1078B01 F93F9138 E2A6382D 28431357 64A6583E
        E5E2E53F 3DA6A97F 7C871BD0 AB5F3E8A EE7C11F2 398D8CC5
        91914622 D590C32A 64D2D536 AC342D10 8455F5DF FAD02D66

MacKey is
                                                 F4F990F3 3337F508
        E32EF04B B4FC6343 E66A81C1 DE1EBC2D A73E6C2F C66FC0F4

Mtag is

```
                        940E1C7F 44A0E4D3 7693BEE7 27EB06DF
        08476849 53C9EFCE 36E8EB06 3A5B250D F6512F29 563553D7
        D1A6E9BE 4EF4C017 D4F95A6C 75C51D3E FC386F98 7AA68B3C


KeyData is
                                                  EA78B1EA E1F8FEB9
        337FA71D 404B30E7 4B064E66 2F12B477 DC88A267 74379248
        84874659 A63374D6 25BA8922 0758992D DB88CCD1 A6E03FD9
        78B4C48A 361C4FD6 D39C0C9D DCDFBFCC E13B9DDD 8E0AE94E
        ECC7E6EE 81C09AF2 BFD22BC4 89171818 997C54F2 53EC81C6
        111AE8E5 70556882 76D23A42 EBC09714 98EE0850 89DC789D




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Zs is
        04E6EA7E EB79EE4B EFFDF2E6 E264A1E9 E4C309E7 5C5FA4C4
        517BFEEE 7D64F383 227A1FE2 75F10B0C D182638E 5AD75CD8
        4A7331D0 2AD199BE ECDC6756 EC094CE6 476B78C9 3AC8C02D


Ze is
        0534AAF3 25606A84 324A0E34 CFF02963 D125470F 92BA808D
        CEA30098 A4A8FD27 AFB134CE 22919C3E 02C5D19E 4676C5F2
        929A23B2 4B016F08 C99E7240 3FB59AD6 82D9B9EA A0D449A8


Z is
        0534AAF3 25606A84 324A0E34 CFF02963 D125470F 92BA808D
        CEA30098 A4A8FD27 AFB134CE 22919C3E 02C5D19E 4676C5F2
        929A23B2 4B016F08 C99E7240 3FB59AD6 82D9B9EA A0D449A8
        04E6EA7E EB79EE4B EFFDF2E6 E264A1E9 E4C309E7 5C5FA4C4
        517BFEEE 7D64F383 227A1FE2 75F10B0C D182638E 5AD75CD8
        4A7331D0 2AD199BE ECDC6756 EC094CE6 476B78C9 3AC8C02D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                        F4F990F3 3337F508 E32EF04B B4FC6343
        E66A81C1 DE1EBC2D A73E6C2F C66FC0F4 EA78B1EA E1F8FEB9
```

```
        337FA71D 404B30E7 4B064E66 2F12B477 DC88A267 74379248
        84874659 A63374D6 25BA8922 0758992D DB88CCD1 A6E03FD9
        78B4C48A 361C4FD6 D39C0C9D DCDFBFCC E13B9DDD 8E0AE94E
        ECC7E6EE 81C09AF2 BFD22BC4 89171818 997C54F2 53EC81C6
        111AE8E5 70556882 76D23A42 EBC09714 98EE0850 89DC789D


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        0121E5C2 A9941CE7 4E7C7F6C 19247594 D9A29A06 FEE2ED16
        6947EBF2 090985BC 87BB3E0F B787B504 F125E780 143B7C7C
        110D3493 5BBBC05A D1CA0083 4F6FF877 40C15AA8 D097D03C
        0426B4CC D1078B01 F93F9138 E2A6382D 28431357 64A6583E
        E5E2E53F 3DA6A97F 7C871BD0 AB5F3E8A EE7C11F2 398D8CC5
        91914622 D590C32A 64D2D536 AC342D10 8455F5DF FAD02D66
        0669AE9D 0C657ED8 5B6174DD FC33F02E 2A28B422 5A0BE50B
        DB8303E1 CFCEFFCC F113D6FA 07EEA236 E0E72BDE F678D424
        28CC0379 85DE19D4 E3BAF9A7 0B793CCD 0BC8E2EF E1AF5993
        00D54789 9C67ED17 B5F8997E 0D119729 2D06062A 8E7E7459
        CE620B0A C3F633BD 4A8AF428 59A1B0F9 53193CA3 062D310D
        9620B72C CD1B0A68 B34E9DA0 AD18BA34 48140686 8A2A57F5


MacKey is
                                                F4F990F3 3337F508
        E32EF04B B4FC6343 E66A81C1 DE1EBC2D A73E6C2F C66FC0F4


Mtag is
                         22320DB2 C9E3763B 85E60E91 F526B485
        5D516C7F 15059293 F95E86F5 C90CAD04 D405A378 83333CE1
        5DA59C78 8817E241 744E9AC4 40212BB1 AA4BBF86 4C9E7BFD


KeyData is
                                                EA78B1EA E1F8FEB9
        337FA71D 404B30E7 4B064E66 2F12B477 DC88A267 74379248
        84874659 A63374D6 25BA8922 0758992D DB88CCD1 A6E03FD9
        78B4C48A 361C4FD6 D39C0C9D DCDFBFCC E13B9DDD 8E0AE94E
        ECC7E6EE 81C09AF2 BFD22BC4 89171818 997C54F2 53EC81C6
        111AE8E5 70556882 76D23A42 EBC09714 98EE0850 89DC789D



-----------------------------------------------------------
```

```
Scheme Initiator, Key Confirmation Bilateral
Zs is
        04E6EA7E EB79EE4B EFFDF2E6 E264A1E9 E4C309E7 5C5FA4C4
        517BFEEE 7D64F383 227A1FE2 75F10B0C D182638E 5AD75CD8
        4A7331D0 2AD199BE ECDC6756 EC094CE6 476B78C9 3AC8C02D


Ze is
        0534AAF3 25606A84 324A0E34 CFF02963 D125470F 92BA808D
        CEA30098 A4A8FD27 AFB134CE 22919C3E 02C5D19E 4676C5F2
        929A23B2 4B016F08 C99E7240 3FB59AD6 82D9B9EA A0D449A8


Z is
        0534AAF3 25606A84 324A0E34 CFF02963 D125470F 92BA808D
        CEA30098 A4A8FD27 AFB134CE 22919C3E 02C5D19E 4676C5F2
        929A23B2 4B016F08 C99E7240 3FB59AD6 82D9B9EA A0D449A8
        04E6EA7E EB79EE4B EFFDF2E6 E264A1E9 E4C309E7 5C5FA4C4
        517BFEEE 7D64F383 227A1FE2 75F10B0C D182638E 5AD75CD8
        4A7331D0 2AD199BE ECDC6756 EC094CE6 476B78C9 3AC8C02D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         F4F990F3 3337F508 E32EF04B B4FC6343
        E66A81C1 DE1EBC2D A73E6C2F C66FC0F4 EA78B1EA E1F8FEB9
        337FA71D 404B30E7 4B064E66 2F12B477 DC88A267 74379248
        84874659 A63374D6 25BA8922 0758992D DB88CCD1 A6E03FD9
        78B4C48A 361C4FD6 D39C0C9D DCDFBFCC E13B9DDD 8E0AE94E
        ECC7E6EE 81C09AF2 BFD22BC4 89171818 997C54F2 53EC81C6
        111AE8E5 70556882 76D23A42 EBC09714 98EE0850 89DC789D


U2V
----------------
MacData is
                         4B435F32 5F55414C 49434542 4F424259
        0669AE9D 0C657ED8 5B6174DD FC33F02E 2A28B422 5A0BE50B
        DB8303E1 CFCEFFCC F113D6FA 07EEA236 E0E72BDE F678D424
        28CC0379 85DE19D4 E3BAF9A7 0B793CCD 0BC8E2EF E1AF5993
        00D54789 9C67ED17 B5F8997E 0D119729 2D06062A 8E7E7459
        CE620B0A C3F633BD 4A8AF428 59A1B0F9 53193CA3 062D310D
        9620B72C CD1B0A68 B34E9DA0 AD18BA34 48140686 8A2A57F5
```

```
        0121E5C2 A9941CE7 4E7C7F6C 19247594 D9A29A06 FEE2ED16
        6947EBF2 090985BC 87BB3E0F B787B504 F125E780 143B7C7C
        110D3493 5BBBC05A D1CA0083 4F6FF877 40C15AA8 D097D03C
        0426B4CC D1078B01 F93F9138 E2A6382D 28431357 64A6583E
        E5E2E53F 3DA6A97F 7C871BD0 AB5F3E8A EE7C11F2 398D8CC5
        91914622 D590C32A 64D2D536 AC342D10 8455F5DF FAD02D66


MacKey is
                                            F4F990F3 3337F508
        E32EF04B B4FC6343 E66A81C1 DE1EBC2D A73E6C2F C66FC0F4


Mtag is
                         501B10FB EB7CED18 258FA16A D76733C3
        52552DB1 68D0A1AC 9540F989 C3583089 44531837 BD42F312
        973E3E5B 8ADDF7BF 8D2C1644 DC39FFCC 5FD3E212 03A01CFA


V2U
----------------
MacData is
                         4B435F32 5F56424F 42425941 4C494345
        0121E5C2 A9941CE7 4E7C7F6C 19247594 D9A29A06 FEE2ED16
        6947EBF2 090985BC 87BB3E0F B787B504 F125E780 143B7C7C
        110D3493 5BBBC05A D1CA0083 4F6FF877 40C15AA8 D097D03C
        0426B4CC D1078B01 F93F9138 E2A6382D 28431357 64A6583E
        E5E2E53F 3DA6A97F 7C871BD0 AB5F3E8A EE7C11F2 398D8CC5
        91914622 D590C32A 64D2D536 AC342D10 8455F5DF FAD02D66
        0669AE9D 0C657ED8 5B6174DD FC33F02E 2A28B422 5A0BE50B
        DB8303E1 CFCEFFCC F113D6FA 07EEA236 E0E72BDE F678D424
        28CC0379 85DE19D4 E3BAF9A7 0B793CCD 0BC8E2EF E1AF5993
        00D54789 9C67ED17 B5F8997E 0D119729 2D06062A 8E7E7459
        CE620B0A C3F633BD 4A8AF428 59A1B0F9 53193CA3 062D310D
        9620B72C CD1B0A68 B34E9DA0 AD18BA34 48140686 8A2A57F5


MacKey is
                                            F4F990F3 3337F508
        E32EF04B B4FC6343 E66A81C1 DE1EBC2D A73E6C2F C66FC0F4


Mtag is
                         BC1FCD85 9AC09F48 D49DE1DF C938699A
        FBAC2558 A8AD9891 1625CDAF D862BD42 31CCAEAC E5AB9CE1
        C6239B5D 5360BCA3 875EDA99 AB06A044 5E8C880F 0D67BBC2
```

KeyData is
                                                EA78B1EA E1F8FEB9
        337FA71D 404B30E7 4B064E66 2F12B477 DC88A267 74379248
        84874659 A63374D6 25BA8922 0758992D DB88CCD1 A6E03FD9
        78B4C48A 361C4FD6 D39C0C9D DCDFBFCC E13B9DDD 8E0AE94E
        ECC7E6EE 81C09AF2 BFD22BC4 89171818 997C54F2 53EC81C6
        111AE8E5 70556882 76D23A42 EBC09714 98EE0850 89DC789D

FullMQV(K-571)
----
dsU is
        009B592D 32F99420 05A38021 D26E7AA6 ED3E78BB DFF2A861
        311B89C9 9DF67762 8EE47F3D 71AE14C6 6EDF0B6C 474E6AA6
        92A4B5BF 3D0814BB 28F38344 D445A44E 5E5FEFBC 3C00978C

QsU_x is
        04F6BD3B 3800DEAF 6D729E0C 29320D34 9E0EFDB5 D74352FD
        DD7EBA85 0BCB04A9 D699EEEB F4204910 7FB65ED4 60CD36B8
        376E0946 56C72747 1BC9982C D5F6E4A8 BDF941DC 1194915B

QsU_y is
        02FD71C0 43003170 0BADD2FC 922C037D 1EABB673 481FE607
        93F1D296 BD59A52B 9A4358BE 99D858DB BECE5240 4358FA17
        9F18D497 E41C3EC4 59D78F2A 2C6F0EDA CC353AD8 59667EAB

dsV is
        01823854 AF10876C 19AEE8EC 6691AD9E 7E294860 5347F7DF
        0EB770FE EB2E71B9 8FAB326F FAEDFEE6 7093A304 8B79CA07
        C7A718DD 32DE5305 48D0FD9B 553AFC00 0E927766 61F71FBB

QsV_x is
        04C74E10 D370016A 080BEDD0 E852F986 EFC63CAC 08BF055C
        795CD634 DF8BEB7A 4411AB19 358E58AC 8000F22F 9528F4E1
        CBF128B6 B5871363 4D62415E BFCD5A5A 94653F8D FDF0703B

QsV_y is

06E73204 610FA3AC B35DD890 F03D2E5C 9BFA20DD 29DA26B6
4B13DEC6 399061A2 DB2BBB0B 6CCF848C 6567B5FA 220AB1B8
2A70DF20 F2B4105B DA8520C2 02BF828A 56A67DDC B9E79B24

deU is
013AC597 40DDBC84 E4803312 4D269467 71CC4872 706EF9F6
34CE0E8A F1A227E8 E14A088E 9B274ADD 07249E3B 8FC69719
10EDE19F 15F9CF94 6BF59829 1F372BD0 7CE0824B 40E5B486

QeU_x is
0669AE9D 0C657ED8 5B6174DD FC33F02E 2A28B422 5A0BE50B
DB8303E1 CFCEFFCC F113D6FA 07EEA236 E0E72BDE F678D424
28CC0379 85DE19D4 E3BAF9A7 0B793CCD 0BC8E2EF E1AF5993

QeU_y is
00D54789 9C67ED17 B5F8997E 0D119729 2D06062A 8E7E7459
CE620B0A C3F633BD 4A8AF428 59A1B0F9 53193CA3 062D310D
9620B72C CD1B0A68 B34E9DA0 AD18BA34 48140686 8A2A57F5

deV is
0035076B C0FAE543 F8E32E41 3BD442A5 4EF489B8 9927B021
0360F83F 8703C448 C72F4550 D6460FDD 1E576438 A072A2B1
CD4477B6 F0D61E5F 6A9D281C 9A4BBB5F 14E13C1C 7C0500CD

QeV_x is
0121E5C2 A9941CE7 4E7C7F6C 19247594 D9A29A06 FEE2ED16
6947EBF2 090985BC 87BB3E0F B787B504 F125E780 143B7C7C
110D3493 5BBBC05A D1CA0083 4F6FF877 40C15AA8 D097D03C

QeV_y is
0426B4CC D1078B01 F93F9138 E2A6382D 28431357 64A6583E
E5E2E53F 3DA6A97F 7C871BD0 AB5F3E8A EE7C11F2 398D8CC5
91914622 D590C32A 64D2D536 AC342D10 8455F5DF FAD02D66

---

no Key Confirmation
Z is

```
        04F2E552 5F5FA69D A34C052F 4E58688E 47CA683A 339D7B03
        B10811C8 FE939E06 61729F71 4F5C7D76 3E201F27 E4B28F0C
        38F827A2 36E9656E 58E90033 E478BE17 78B01613 AA058E99


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                            7DB4C1F7 2819F363
        F7D48097 6ED9E6E7 B77BF1C2 51D68D17 B473F067 A05A5970
        5FDB6838 6F8E1D96 4B5FF24D AEA4BB64 512ECFB8 14A67BA3
        C09205BA 39B33782 1FE481D4 35E7DDE7 D9ABC145 2B7874F5
        B0E9243F 11B69EA2 92C2BACB CFA8AC82 A38C6EAE DA267F5B
        2407BAA6 AD40F428 C765C3C1 2168CCBB F650BECB 383B020D


KeyData is
                                            7DB4C1F7 2819F363
        F7D48097 6ED9E6E7 B77BF1C2 51D68D17 B473F067 A05A5970
        5FDB6838 6F8E1D96 4B5FF24D AEA4BB64 512ECFB8 14A67BA3
        C09205BA 39B33782 1FE481D4 35E7DDE7 D9ABC145 2B7874F5
        B0E9243F 11B69EA2 92C2BACB CFA8AC82 A38C6EAE DA267F5B
        2407BAA6 AD40F428 C765C3C1 2168CCBB F650BECB 383B020D




-------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Z is
        04F2E552 5F5FA69D A34C052F 4E58688E 47CA683A 339D7B03
        B10811C8 FE939E06 61729F71 4F5C7D76 3E201F27 E4B28F0C
        38F827A2 36E9656E 58E90033 E478BE17 78B01613 AA058E99


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                            7DB4C1F7 2819F363 F7D48097 6ED9E6E7
        B77BF1C2 51D68D17 B473F067 A05A5970 5FDB6838 6F8E1D96
        4B5FF24D AEA4BB64 512ECFB8 14A67BA3 C09205BA 39B33782
        1FE481D4 35E7DDE7 D9ABC145 2B7874F5 B0E9243F 11B69EA2
```

92C2BACB CFA8AC82 A38C6EAE DA267F5B 2407BAA6 AD40F428
C765C3C1 2168CCBB F650BECB 383B020D DF26C8DA 7F32B00B
675AD96D 8D66F964 CC2FB89F 6ED04A31 A807CD28 D493B11B

MacData is
4B435F31 5F55414C 49434542 4F424259
0669AE9D 0C657ED8 5B6174DD FC33F02E 2A28B422 5A0BE50B
DB8303E1 CFCEFFCC F113D6FA 07EEA236 E0E72BDE F678D424
28CC0379 85DE19D4 E3BAF9A7 0B793CCD 0BC8E2EF E1AF5993
00D54789 9C67ED17 B5F8997E 0D119729 2D06062A 8E7E7459
CE620B0A C3F633BD 4A8AF428 59A1B0F9 53193CA3 062D310D
9620B72C CD1B0A68 B34E9DA0 AD18BA34 48140686 8A2A57F5
0121E5C2 A9941CE7 4E7C7F6C 19247594 D9A29A06 FEE2ED16
6947EBF2 090985BC 87BB3E0F B787B504 F125E780 143B7C7C
110D3493 5BBBC05A D1CA0083 4F6FF877 40C15AA8 D097D03C
0426B4CC D1078B01 F93F9138 E2A6382D 28431357 64A6583E
E5E2E53F 3DA6A97F 7C871BD0 AB5F3E8A EE7C11F2 398D8CC5
91914622 D590C32A 64D2D536 AC342D10 8455F5DF FAD02D66

MacKey is
7DB4C1F7 2819F363
F7D48097 6ED9E6E7 B77BF1C2 51D68D17 B473F067 A05A5970

Mtag is
324BFF9D 3AE28186 7C14397D A79E4BE1
FCC2A2D3 F78C77AF 765522E5 BB70A511 2871F399 4BB36AFF
257861CE C8D060C9 6123F712 56ED8667 1EB6B08D 1B532C0A

KeyData is
5FDB6838 6F8E1D96
4B5FF24D AEA4BB64 512ECFB8 14A67BA3 C09205BA 39B33782
1FE481D4 35E7DDE7 D9ABC145 2B7874F5 B0E9243F 11B69EA2
92C2BACB CFA8AC82 A38C6EAE DA267F5B 2407BAA6 AD40F428
C765C3C1 2168CCBB F650BECB 383B020D DF26C8DA 7F32B00B
675AD96D 8D66F964 CC2FB89F 6ED04A31 A807CD28 D493B11B

Scheme Responder, Key Confirmation Provider: V to U
Z is

```
        04F2E552 5F5FA69D A34C052F 4E58688E 47CA683A 339D7B03
        B10811C8 FE939E06 61729F71 4F5C7D76 3E201F27 E4B28F0C
        38F827A2 36E9656E 58E90033 E478BE17 78B01613 AA058E99


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         7DB4C1F7 2819F363 F7D48097 6ED9E6E7
        B77BF1C2 51D68D17 B473F067 A05A5970 5FDB6838 6F8E1D96
        4B5FF24D AEA4BB64 512ECFB8 14A67BA3 C09205BA 39B33782
        1FE481D4 35E7DDE7 D9ABC145 2B7874F5 B0E9243F 11B69EA2
        92C2BACB CFA8AC82 A38C6EAE DA267F5B 2407BAA6 AD40F428
        C765C3C1 2168CCBB F650BECB 383B020D DF26C8DA 7F32B00B
        675AD96D 8D66F964 CC2FB89F 6ED04A31 A807CD28 D493B11B


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        0121E5C2 A9941CE7 4E7C7F6C 19247594 D9A29A06 FEE2ED16
        6947EBF2 090985BC 87BB3E0F B787B504 F125E780 143B7C7C
        110D3493 5BBBC05A D1CA0083 4F6FF877 40C15AA8 D097D03C
        0426B4CC D1078B01 F93F9138 E2A6382D 28431357 64A6583E
        E5E2E53F 3DA6A97F 7C871BD0 AB5F3E8A EE7C11F2 398D8CC5
        91914622 D590C32A 64D2D536 AC342D10 8455F5DF FAD02D66
        0669AE9D 0C657ED8 5B6174DD FC33F02E 2A28B422 5A0BE50B
        DB8303E1 CFCEFFCC F113D6FA 07EEA236 E0E72BDE F678D424
        28CC0379 85DE19D4 E3BAF9A7 0B793CCD 0BC8E2EF E1AF5993
        00D54789 9C67ED17 B5F8997E 0D119729 2D06062A 8E7E7459
        CE620B0A C3F633BD 4A8AF428 59A1B0F9 53193CA3 062D310D
        9620B72C CD1B0A68 B34E9DA0 AD18BA34 48140686 8A2A57F5


MacKey is
                                            7DB4C1F7 2819F363
        F7D48097 6ED9E6E7 B77BF1C2 51D68D17 B473F067 A05A5970


Mtag is
                         9670E54B 38E34E25 B6FCE562 DD56CFA9
        A76861F1 1B6DA598 334087B4 17D2DB43 607386C2 ACE41A41
        7695E2DA 61D0695F B912D3FC 268EB4CA 0457B1C3 03322241
```

```
KeyData is
                                                5FDB6838 6F8E1D96
        4B5FF24D AEA4BB64 512ECFB8 14A67BA3 C09205BA 39B33782
        1FE481D4 35E7DDE7 D9ABC145 2B7874F5 B0E9243F 11B69EA2
        92C2BACB CFA8AC82 A38C6EAE DA267F5B 2407BAA6 AD40F428
        C765C3C1 2168CCBB F650BECB 383B020D DF26C8DA 7F32B00B
        675AD96D 8D66F964 CC2FB89F 6ED04A31 A807CD28 D493B11B



------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
Z is
        04F2E552 5F5FA69D A34C052F 4E58688E 47CA683A 339D7B03
        B10811C8 FE939E06 61729F71 4F5C7D76 3E201F27 E4B28F0C
        38F827A2 36E9656E 58E90033 E478BE17 78B01613 AA058E99


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         7DB4C1F7 2819F363 F7D48097 6ED9E6E7
        B77BF1C2 51D68D17 B473F067 A05A5970 5FDB6838 6F8E1D96
        4B5FF24D AEA4BB64 512ECFB8 14A67BA3 C09205BA 39B33782
        1FE481D4 35E7DDE7 D9ABC145 2B7874F5 B0E9243F 11B69EA2
        92C2BACB CFA8AC82 A38C6EAE DA267F5B 2407BAA6 AD40F428
        C765C3C1 2168CCBB F650BECB 383B020D DF26C8DA 7F32B00B
        675AD96D 8D66F964 CC2FB89F 6ED04A31 A807CD28 D493B11B


U2V
----------------
MacData is
                         4B435F32 5F55414C 49434542 4F424259
        0669AE9D 0C657ED8 5B6174DD FC33F02E 2A28B422 5A0BE50B
        DB8303E1 CFCEFFCC F113D6FA 07EEA236 E0E72BDE F678D424
        28CC0379 85DE19D4 E3BAF9A7 0B793CCD 0BC8E2EF E1AF5993
        00D54789 9C67ED17 B5F8997E 0D119729 2D06062A 8E7E7459
        CE620B0A C3F633BD 4A8AF428 59A1B0F9 53193CA3 062D310D
        9620B72C CD1B0A68 B34E9DA0 AD18BA34 48140686 8A2A57F5
        0121E5C2 A9941CE7 4E7C7F6C 19247594 D9A29A06 FEE2ED16
        6947EBF2 090985BC 87BB3E0F B787B504 F125E780 143B7C7C
```

```
        110D3493 5BBBC05A D1CA0083 4F6FF877 40C15AA8 D097D03C
        0426B4CC D1078B01 F93F9138 E2A6382D 28431357 64A6583E
        E5E2E53F 3DA6A97F 7C871BD0 AB5F3E8A EE7C11F2 398D8CC5
        91914622 D590C32A 64D2D536 AC342D10 8455F5DF FAD02D66


MacKey is
                                            7DB4C1F7 2819F363
        F7D48097 6ED9E6E7 B77BF1C2 51D68D17 B473F067 A05A5970


Mtag is
                        12EF4895 159C9928 80BD8D0F D87E6C27
        E5F4AFBC 0FF8E306 9A3FB609 54C8C6A0 FE64B30E 77445107
        02D2CDFE B9394573 19D3582F 720992B7 D72EC453 02851346


V2U
----------------
MacData is
                        4B435F32 5F56424F 42425941 4C494345
        0121E5C2 A9941CE7 4E7C7F6C 19247594 D9A29A06 FEE2ED16
        6947EBF2 090985BC 87BB3E0F B787B504 F125E780 143B7C7C
        110D3493 5BBBC05A D1CA0083 4F6FF877 40C15AA8 D097D03C
        0426B4CC D1078B01 F93F9138 E2A6382D 28431357 64A6583E
        E5E2E53F 3DA6A97F 7C871BD0 AB5F3E8A EE7C11F2 398D8CC5
        91914622 D590C32A 64D2D536 AC342D10 8455F5DF FAD02D66
        0669AE9D 0C657ED8 5B6174DD FC33F02E 2A28B422 5A0BE50B
        DB8303E1 CFCEFFCC F113D6FA 07EEA236 E0E72BDE F678D424
        28CC0379 85DE19D4 E3BAF9A7 0B793CCD 0BC8E2EF E1AF5993
        00D54789 9C67ED17 B5F8997E 0D119729 2D06062A 8E7E7459
        CE620B0A C3F633BD 4A8AF428 59A1B0F9 53193CA3 062D310D
        9620B72C CD1B0A68 B34E9DA0 AD18BA34 48140686 8A2A57F5


MacKey is
                                            7DB4C1F7 2819F363
        F7D48097 6ED9E6E7 B77BF1C2 51D68D17 B473F067 A05A5970


Mtag is
                        075FD7AB 8940505F 0A4CC9D7 80902202
        C53ED1CD 7D1554E6 CC6C2BA3 62DE042E 856820F4 ECD7AA9B
        1BBEE468 6B6F0B6E 2A84CC0E FA9F5A6A 70B6319C 42DB7CA0
```

```
KeyData is
                                                5FDB6838 6F8E1D96
        4B5FF24D AEA4BB64 512ECFB8 14A67BA3 C09205BA 39B33782
        1FE481D4 35E7DDE7 D9ABC145 2B7874F5 B0E9243F 11B69EA2
        92C2BACB CFA8AC82 A38C6EAE DA267F5B 2407BAA6 AD40F428
        C765C3C1 2168CCBB F650BECB 383B020D DF26C8DA 7F32B00B
        675AD96D 8D66F964 CC2FB89F 6ED04A31 A807CD28 D493B11B



EphemeralUnifiedCDH(K-571)
-----------------------------------------------------------
deU is
        013AC597 40DDBC84 E4803312 4D269467 71CC4872 706EF9F6
        34CE0E8A F1A227E8 E14A088E 9B274ADD 07249E3B 8FC69719
        10EDE19F 15F9CF94 6BF59829 1F372BD0 7CE0824B 40E5B486


QeU_x is
        0669AE9D 0C657ED8 5B6174DD FC33F02E 2A28B422 5A0BE50B
        DB8303E1 CFCEFFCC F113D6FA 07EEA236 E0E72BDE F678D424
        28CC0379 85DE19D4 E3BAF9A7 0B793CCD 0BC8E2EF E1AF5993


QeU_y is
        00D54789 9C67ED17 B5F8997E 0D119729 2D06062A 8E7E7459
        CE620B0A C3F633BD 4A8AF428 59A1B0F9 53193CA3 062D310D
        9620B72C CD1B0A68 B34E9DA0 AD18BA34 48140686 8A2A57F5


deV is
        0035076B C0FAE543 F8E32E41 3BD442A5 4EF489B8 9927B021
        0360F83F 8703C448 C72F4550 D6460FDD 1E576438 A072A2B1
        CD4477B6 F0D61E5F 6A9D281C 9A4BBB5F 14E13C1C 7C0500CD


QeV_x is
        0121E5C2 A9941CE7 4E7C7F6C 19247594 D9A29A06 FEE2ED16
        6947EBF2 090985BC 87BB3E0F B787B504 F125E780 143B7C7C
        110D3493 5BBBC05A D1CA0083 4F6FF877 40C15AA8 D097D03C


QeV_y is
        0426B4CC D1078B01 F93F9138 E2A6382D 28431357 64A6583E
        E5E2E53F 3DA6A97F 7C871BD0 AB5F3E8A EE7C11F2 398D8CC5
```

```
        91914622 D590C32A 64D2D536 AC342D10 8455F5DF FAD02D66



-------------------------------------------------------------
no Key Confirmation
Z is
        0534AAF3 25606A84 324A0E34 CFF02963 D125470F 92BA808D
        CEA30098 A4A8FD27 AFB134CE 22919C3E 02C5D19E 4676C5F2
        929A23B2 4B016F08 C99E7240 3FB59AD6 82D9B9EA A0D449A8


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                            6B587FF2 DEC16CA4
        8BFC8EF1 3044E113 63D793D5 322AB6F2 EB08128F 35CF1A73
        6B4F625A 8B7D0152 2EC53BF9 F31D435C C9831D85 50815DF2
        B0869953 ED94BC6A D7EE9EFC C36E6BD1 0BADCC55 42C97198
        345AC416 86E0DFEC 298887EE 13AD44CB 7CD67E57 D9985222
        F3BF8D88 562F40CE 9E6B102C 9D9C8A7B 9FFC1FF8 165D1F80


KeyData is
                                            6B587FF2 DEC16CA4
        8BFC8EF1 3044E113 63D793D5 322AB6F2 EB08128F 35CF1A73
        6B4F625A 8B7D0152 2EC53BF9 F31D435C C9831D85 50815DF2
        B0869953 ED94BC6A D7EE9EFC C36E6BD1 0BADCC55 42C97198
        345AC416 86E0DFEC 298887EE 13AD44CB 7CD67E57 D9985222
        F3BF8D88 562F40CE 9E6B102C 9D9C8A7B 9FFC1FF8 165D1F80




OnePassUnifiedCDH(K-571)
-------------------------------------------------------------
dsU is
        009B592D 32F99420 05A38021 D26E7AA6 ED3E78BB DFF2A861
        311B89C9 9DF67762 8EE47F3D 71AE14C6 6EDF0B6C 474E6AA6
        92A4B5BF 3D0814BB 28F38344 D445A44E 5E5FEFBC 3C00978C


QsU_x is
```

04F6BD3B 3800DEAF 6D729E0C 29320D34 9E0EFDB5 D74352FD
DD7EBA85 0BCB04A9 D699EEEB F4204910 7FB65ED4 60CD36B8
376E0946 56C72747 1BC9982C D5F6E4A8 BDF941DC 1194915B

QsU_y is
02FD71C0 43003170 0BADD2FC 922C037D 1EABB673 481FE607
93F1D296 BD59A52B 9A4358BE 99D858DB BECE5240 4358FA17
9F18D497 E41C3EC4 59D78F2A 2C6F0EDA CC353AD8 59667EAB

dsV is
01823854 AF10876C 19AEE8EC 6691AD9E 7E294860 5347F7DF
0EB770FE EB2E71B9 8FAB326F FAEDFEE6 7093A304 8B79CA07
C7A718DD 32DE5305 48D0FD9B 553AFC00 0E927766 61F71FBB

QsV_x is
04C74E10 D370016A 080BEDD0 E852F986 EFC63CAC 08BF055C
795CD634 DF8BEB7A 4411AB19 358E58AC 8000F22F 9528F4E1
CBF128B6 B5871363 4D62415E BFCD5A5A 94653F8D FDF0703B

QsV_y is
06E73204 610FA3AC B35DD890 F03D2E5C 9BFA20DD 29DA26B6
4B13DEC6 399061A2 DB2BBB0B 6CCF848C 6567B5FA 220AB1B8
2A70DF20 F2B4105B DA8520C2 02BF828A 56A67DDC B9E79B24

deU is
013AC597 40DDBC84 E4803312 4D269467 71CC4872 706EF9F6
34CE0E8A F1A227E8 E14A088E 9B274ADD 07249E3B 8FC69719
10EDE19F 15F9CF94 6BF59829 1F372BD0 7CE0824B 40E5B486

QeU_x is
0669AE9D 0C657ED8 5B6174DD FC33F02E 2A28B422 5A0BE50B
DB8303E1 CFCEFFCC F113D6FA 07EEA236 E0E72BDE F678D424
28CC0379 85DE19D4 E3BAF9A7 0B793CCD 0BC8E2EF E1AF5993

QeU_y is
00D54789 9C67ED17 B5F8997E 0D119729 2D06062A 8E7E7459
CE620B0A C3F633BD 4A8AF428 59A1B0F9 53193CA3 062D310D
9620B72C CD1B0A68 B34E9DA0 AD18BA34 48140686 8A2A57F5

```
-----------------------------------------------------------
no Key Confirmation
Zs is
        04E6EA7E EB79EE4B EFFDF2E6 E264A1E9 E4C309E7 5C5FA4C4
        517BFEEE 7D64F383 227A1FE2 75F10B0C D182638E 5AD75CD8
        4A7331D0 2AD199BE ECDC6756 EC094CE6 476B78C9 3AC8C02D


Ze is
        05F36BAF 06996B30 AF14EE01 E92CC6A7 2D15CFBA F32F22AC
        946C496D 46A89D95 93CB1872 6A087E7E 4268DBFE ABC0F806
        3A208335 11025BB7 47210411 D2EE1AC1 C89E68EA 566AAA37


Z is
        05F36BAF 06996B30 AF14EE01 E92CC6A7 2D15CFBA F32F22AC
        946C496D 46A89D95 93CB1872 6A087E7E 4268DBFE ABC0F806
        3A208335 11025BB7 47210411 D2EE1AC1 C89E68EA 566AAA37
        04E6EA7E EB79EE4B EFFDF2E6 E264A1E9 E4C309E7 5C5FA4C4
        517BFEEE 7D64F383 227A1FE2 75F10B0C D182638E 5AD75CD8
        4A7331D0 2AD199BE ECDC6756 EC094CE6 476B78C9 3AC8C02D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                            89F200C1 354FFB13
        5C130869 C22E9855 2432A89B EB411438 BFE36865 61F67E64
        2F51634B 21595C99 A05C54F3 8B65AD9E CDFEC15E 64EC9CCE
        B7DE0C96 52901647 28CD3948 7BF8D2CC F807288E 3BEF1A01
        9D3BA89E A56BA96C D38DA82D F1044BB3 3275DD72 B6261674
        7ADB0F3C 51670F41 E1979F57 D9196F3E 97CCCCC8 886429C8


KeyData is
                                            89F200C1 354FFB13
        5C130869 C22E9855 2432A89B EB411438 BFE36865 61F67E64
        2F51634B 21595C99 A05C54F3 8B65AD9E CDFEC15E 64EC9CCE
        B7DE0C96 52901647 28CD3948 7BF8D2CC F807288E 3BEF1A01
        9D3BA89E A56BA96C D38DA82D F1044BB3 3275DD72 B6261674
        7ADB0F3C 51670F41 E1979F57 D9196F3E 97CCCCC8 886429C8
```

```
-------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB72 9216428C AAB82B22 AC7C3B0A
        F6149001 A1AE5EEA A5B08ABE D40B0946 203F5156 8BBA3866


Zs is
        04E6EA7E EB79EE4B EFFDF2E6 E264A1E9 E4C309E7 5C5FA4C4
        517BFEEE 7D64F383 227A1FE2 75F10B0C D182638E 5AD75CD8
        4A7331D0 2AD199BE ECDC6756 EC094CE6 476B78C9 3AC8C02D


Ze is
        05F36BAF 06996B30 AF14EE01 E92CC6A7 2D15CFBA F32F22AC
        946C496D 46A89D95 93CB1872 6A087E7E 4268DBFE ABC0F806
        3A208335 11025BB7 47210411 D2EE1AC1 C89E68EA 566AAA37


Z is
        05F36BAF 06996B30 AF14EE01 E92CC6A7 2D15CFBA F32F22AC
        946C496D 46A89D95 93CB1872 6A087E7E 4268DBFE ABC0F806
        3A208335 11025BB7 47210411 D2EE1AC1 C89E68EA 566AAA37
        04E6EA7E EB79EE4B EFFDF2E6 E264A1E9 E4C309E7 5C5FA4C4
        517BFEEE 7D64F383 227A1FE2 75F10B0C D182638E 5AD75CD8
        4A7331D0 2AD199BE ECDC6756 EC094CE6 476B78C9 3AC8C02D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         89F200C1 354FFB13 5C130869 C22E9855
        2432A89B EB411438 BFE36865 61F67E64 2F51634B 21595C99
        A05C54F3 8B65AD9E CDFEC15E 64EC9CCE B7DE0C96 52901647
        28CD3948 7BF8D2CC F807288E 3BEF1A01 9D3BA89E A56BA96C
        D38DA82D F1044BB3 3275DD72 B6261674 7ADB0F3C 51670F41
        E1979F57 D9196F3E 97CCCCC8 886429C8 00AF6264 19250A54
        2F632EB9 4FFFFF77 AE96FAAF 40999F14 28B056B8 959281E1
```

```
MacData is
                        4B435F31 5F55414C 49434542 4F424259
        0669AE9D 0C657ED8 5B6174DD FC33F02E 2A28B422 5A0BE50B
        DB8303E1 CFCEFFCC F113D6FA 07EEA236 E0E72BDE F678D424
        28CC0379 85DE19D4 E3BAF9A7 0B793CCD 0BC8E2EF E1AF5993
        00D54789 9C67ED17 B5F8997E 0D119729 2D06062A 8E7E7459
        CE620B0A C3F633BD 4A8AF428 59A1B0F9 53193CA3 062D310D
        9620B72C CD1B0A68 B34E9DA0 AD18BA34 48140686 8A2A57F5
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB72 9216428C AAB82B22 AC7C3B0A
        F6149001 A1AE5EEA A5B08ABE D40B0946 203F5156 8BBA3866


MacKey is
                                                89F200C1 354FFB13
        5C130869 C22E9855 2432A89B EB411438 BFE36865 61F67E64


Mtag is
                        5D685BE5 12D2E69E 2021FC38 B6BEA12B
        03A2F1F0 8BE6485E 13383B1C 8AB3801E 47FF4CA8 94AE78C9
        07911946 819CCC36 B22AAB0A 95234EA8 E5B670E1 8CEA3CDE


KeyData is
                                                2F51634B 21595C99
        A05C54F3 8B65AD9E CDFEC15E 64EC9CCE B7DE0C96 52901647
        28CD3948 7BF8D2CC F807288E 3BEF1A01 9D3BA89E A56BA96C
        D38DA82D F1044BB3 3275DD72 B6261674 7ADB0F3C 51670F41
        E1979F57 D9196F3E 97CCCCC8 886429C8 00AF6264 19250A54
        2F632EB9 4FFFFF77 AE96FAAF 40999F14 28B056B8 959281E1




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB72 9216428C AAB82B22 AC7C3B0A
        F6149001 A1AE5EEA A5B08ABE D40B0946 203F5156 8BBA3866


Zs is
        04E6EA7E EB79EE4B EFFDF2E6 E264A1E9 E4C309E7 5C5FA4C4
```

517BFEEE 7D64F383 227A1FE2 75F10B0C D182638E 5AD75CD8
4A7331D0 2AD199BE ECDC6756 EC094CE6 476B78C9 3AC8C02D

Ze is
05F36BAF 06996B30 AF14EE01 E92CC6A7 2D15CFBA F32F22AC
946C496D 46A89D95 93CB1872 6A087E7E 4268DBFE ABC0F806
3A208335 11025BB7 47210411 D2EE1AC1 C89E68EA 566AAA37

Z is
05F36BAF 06996B30 AF14EE01 E92CC6A7 2D15CFBA F32F22AC
946C496D 46A89D95 93CB1872 6A087E7E 4268DBFE ABC0F806
3A208335 11025BB7 47210411 D2EE1AC1 C89E68EA 566AAA37
04E6EA7E EB79EE4B EFFDF2E6 E264A1E9 E4C309E7 5C5FA4C4
517BFEEE 7D64F383 227A1FE2 75F10B0C D182638E 5AD75CD8
4A7331D0 2AD199BE ECDC6756 EC094CE6 476B78C9 3AC8C02D

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
89F200C1 354FFB13 5C130869 C22E9855
2432A89B EB411438 BFE36865 61F67E64 2F51634B 21595C99
A05C54F3 8B65AD9E CDFEC15E 64EC9CCE B7DE0C96 52901647
28CD3948 7BF8D2CC F807288E 3BEF1A01 9D3BA89E A56BA96C
D38DA82D F1044BB3 3275DD72 B6261674 7ADB0F3C 51670F41
E1979F57 D9196F3E 97CCCCC8 886429C8 00AF6264 19250A54
2F632EB9 4FFFFF77 AE96FAAF 40999F14 28B056B8 959281E1

MacData is
4B435F31 5F56424F 42425941 4C494345
0669AE9D 0C657ED8 5B6174DD FC33F02E 2A28B422 5A0BE50B
DB8303E1 CFCEFFCC F113D6FA 07EEA236 E0E72BDE F678D424
28CC0379 85DE19D4 E3BAF9A7 0B793CCD 0BC8E2EF E1AF5993
00D54789 9C67ED17 B5F8997E 0D119729 2D06062A 8E7E7459
CE620B0A C3F633BD 4A8AF428 59A1B0F9 53193CA3 062D310D
9620B72C CD1B0A68 B34E9DA0 AD18BA34 48140686 8A2A57F5

MacKey is
89F200C1 354FFB13
5C130869 C22E9855 2432A89B EB411438 BFE36865 61F67E64

```
Mtag is
                        8ECAD346 82962CE8 59973E3A 3361871B
        D03C149A CFE57513 265CE266 867DE358 E9055C14 5671A6D7
        17367E15 2EF39C15 28BF4F69 CD0E782F 1B3088CA EDB291B2


KeyData is
                                                 2F51634B 21595C99
        A05C54F3 8B65AD9E CDFEC15E 64EC9CCE B7DE0C96 52901647
        28CD3948 7BF8D2CC F807288E 3BEF1A01 9D3BA89E A56BA96C
        D38DA82D F1044BB3 3275DD72 B6261674 7ADB0F3C 51670F41
        E1979F57 D9196F3E 97CCCCC8 886429C8 00AF6264 19250A54
        2F632EB9 4FFFFF77 AE96FAAF 40999F14 28B056B8 959281E1




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB72 9216428C AAB82B22 AC7C3B0A
        F6149001 A1AE5EEA A5B08ABE D40B0946 203F5156 8BBA3866


Zs is
        04E6EA7E EB79EE4B EFFDF2E6 E264A1E9 E4C309E7 5C5FA4C4
        517BFEEE 7D64F383 227A1FE2 75F10B0C D182638E 5AD75CD8
        4A7331D0 2AD199BE ECDC6756 EC094CE6 476B78C9 3AC8C02D


Ze is
        05F36BAF 06996B30 AF14EE01 E92CC6A7 2D15CFBA F32F22AC
        946C496D 46A89D95 93CB1872 6A087E7E 4268DBFE ABC0F806
        3A208335 11025BB7 47210411 D2EE1AC1 C89E68EA 566AAA37


Z is
        05F36BAF 06996B30 AF14EE01 E92CC6A7 2D15CFBA F32F22AC
        946C496D 46A89D95 93CB1872 6A087E7E 4268DBFE ABC0F806
        3A208335 11025BB7 47210411 D2EE1AC1 C89E68EA 566AAA37
        04E6EA7E EB79EE4B EFFDF2E6 E264A1E9 E4C309E7 5C5FA4C4
        517BFEEE 7D64F383 227A1FE2 75F10B0C D182638E 5AD75CD8
        4A7331D0 2AD199BE ECDC6756 EC094CE6 476B78C9 3AC8C02D
```

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         89F200C1 354FFB13 5C130869 C22E9855
        2432A89B EB411438 BFE36865 61F67E64 2F51634B 21595C99
        A05C54F3 8B65AD9E CDFEC15E 64EC9CCE B7DE0C96 52901647
        28CD3948 7BF8D2CC F807288E 3BEF1A01 9D3BA89E A56BA96C
        D38DA82D F1044BB3 3275DD72 B6261674 7ADB0F3C 51670F41
        E1979F57 D9196F3E 97CCCCC8 886429C8 00AF6264 19250A54
        2F632EB9 4FFFFF77 AE96FAAF 40999F14 28B056B8 959281E1


U2V
----------------
MacData is
                         4B435F32 5F55414C 49434542 4F424259
        0669AE9D 0C657ED8 5B6174DD FC33F02E 2A28B422 5A0BE50B
        DB8303E1 CFCEFFCC F113D6FA 07EEA236 E0E72BDE F678D424
        28CC0379 85DE19D4 E3BAF9A7 0B793CCD 0BC8E2EF E1AF5993
        00D54789 9C67ED17 B5F8997E 0D119729 2D06062A 8E7E7459
        CE620B0A C3F633BD 4A8AF428 59A1B0F9 53193CA3 062D310D
        9620B72C CD1B0A68 B34E9DA0 AD18BA34 48140686 8A2A57F5
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB72 9216428C AAB82B22 AC7C3B0A
        F6149001 A1AE5EEA A5B08ABE D40B0946 203F5156 8BBA3866


MacKey is
                                                 89F200C1 354FFB13
        5C130869 C22E9855 2432A89B EB411438 BFE36865 61F67E64


Mtag is
                         4C69AE1D B1E53AA0 4297764E DF650C9A
        4830EE8B 3A4D3B30 E695869F 592AAC9B 9F38E7AE C3187D18
        61FDDD38 3150B698 FB803041 F0F2C190 277314D7 9AB4F453


V2U
----------------
MacData is
                         4B435F32 5F56424F 42425941 4C494345
```

```
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB72 9216428C AAB82B22 AC7C3B0A
        F6149001 A1AE5EEA A5B08ABE D40B0946 203F5156 8BBA3866
        0669AE9D 0C657ED8 5B6174DD FC33F02E 2A28B422 5A0BE50B
        DB8303E1 CFCEFFCC F113D6FA 07EEA236 E0E72BDE F678D424
        28CC0379 85DE19D4 E3BAF9A7 0B793CCD 0BC8E2EF E1AF5993
        00D54789 9C67ED17 B5F8997E 0D119729 2D06062A 8E7E7459
        CE620B0A C3F633BD 4A8AF428 59A1B0F9 53193CA3 062D310D
        9620B72C CD1B0A68 B34E9DA0 AD18BA34 48140686 8A2A57F5


MacKey is
                                            89F200C1 354FFB13
        5C130869 C22E9855 2432A89B EB411438 BFE36865 61F67E64


Mtag is
                         0CA920CC 11C6874A 351CCA41 2EF0587D
        9F732CA5 8C2FD0D4 6F5BDEA0 95A04B16 6B1E2C81 AFBAD429
        CA1EE5B2 E073058B 016B6F04 08ED83E0 4D3E8045 8C0E5584


KeyData is
                                            2F51634B 21595C99
        A05C54F3 8B65AD9E CDFEC15E 64EC9CCE B7DE0C96 52901647
        28CD3948 7BF8D2CC F807288E 3BEF1A01 9D3BA89E A56BA96C
        D38DA82D F1044BB3 3275DD72 B6261674 7ADB0F3C 51670F41
        E1979F57 D9196F3E 97CCCCC8 886429C8 00AF6264 19250A54
        2F632EB9 4FFFFF77 AE96FAAF 40999F14 28B056B8 959281E1




OnePassMQV(K-571)
------------------------------------------------------------
dsU is
        009B592D 32F99420 05A38021 D26E7AA6 ED3E78BB DFF2A861
        311B89C9 9DF67762 8EE47F3D 71AE14C6 6EDF0B6C 474E6AA6
        92A4B5BF 3D0814BB 28F38344 D445A44E 5E5FEFBC 3C00978C


QsU_x is
        04F6BD3B 3800DEAF 6D729E0C 29320D34 9E0EFDB5 D74352FD
        DD7EBA85 0BCB04A9 D699EEEB F4204910 7FB65ED4 60CD36B8
        376E0946 56C72747 1BC9982C D5F6E4A8 BDF941DC 1194915B
```

QsU_y is
        02FD71C0 43003170 0BADD2FC 922C037D 1EABB673 481FE607
        93F1D296 BD59A52B 9A4358BE 99D858DB BECE5240 4358FA17
        9F18D497 E41C3EC4 59D78F2A 2C6F0EDA CC353AD8 59667EAB

dsV is
        01823854 AF10876C 19AEE8EC 6691AD9E 7E294860 5347F7DF
        0EB770FE EB2E71B9 8FAB326F FAEDFEE6 7093A304 8B79CA07
        C7A718DD 32DE5305 48D0FD9B 553AFC00 0E927766 61F71FBB

QsV_x is
        04C74E10 D370016A 080BEDD0 E852F986 EFC63CAC 08BF055C
        795CD634 DF8BEB7A 4411AB19 358E58AC 8000F22F 9528F4E1
        CBF128B6 B5871363 4D62415E BFCD5A5A 94653F8D FDF0703B

QsV_y is
        06E73204 610FA3AC B35DD890 F03D2E5C 9BFA20DD 29DA26B6
        4B13DEC6 399061A2 DB2BBB0B 6CCF848C 6567B5FA 220AB1B8
        2A70DF20 F2B4105B DA8520C2 02BF828A 56A67DDC B9E79B24

deU is
        013AC597 40DDBC84 E4803312 4D269467 71CC4872 706EF9F6
        34CE0E8A F1A227E8 E14A088E 9B274ADD 07249E3B 8FC69719
        10EDE19F 15F9CF94 6BF59829 1F372BD0 7CE0824B 40E5B486

QeU_x is
        0669AE9D 0C657ED8 5B6174DD FC33F02E 2A28B422 5A0BE50B
        DB8303E1 CFCEFFCC F113D6FA 07EEA236 E0E72BDE F678D424
        28CC0379 85DE19D4 E3BAF9A7 0B793CCD 0BC8E2EF E1AF5993

QeU_y is
        00D54789 9C67ED17 B5F8997E 0D119729 2D06062A 8E7E7459
        CE620B0A C3F633BD 4A8AF428 59A1B0F9 53193CA3 062D310D
        9620B72C CD1B0A68 B34E9DA0 AD18BA34 48140686 8A2A57F5

---

no Key Confirmation
Z is
        05756A96 5EC4FDDD D076DAD2 B6A4EEAC 7A72AB5A 5D0F9BB1
        8F9DFCF3 DB3F8DD4 02730BB4 7AC00C6C F40BC468 8FBD1EE1
        2B7B83A7 CB163C29 58BBAB27 C69D3F75 6F7BA8AE 7B0EA618

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                                            A31D24C8 BDADF88E
        9499D594 FEB5A945 11A03B91 96ABD0E7 CC365520 3F80927A
        1228D075 D434951A 9C678664 7D3AB62A 2B297263 82D92BA4
        36FFBFB0 A0A3FF7C A9932281 C183144E 631856A8 3BBE7588
        ACF1F6E5 1A4B1E76 480BC60C 5551EBC4 B6916580 4DB5AD25
        A5D7E9A5 BF184492 FB9EA6A7 479D586B 44F786BD 8A4F0228

KeyData is
                                            A31D24C8 BDADF88E
        9499D594 FEB5A945 11A03B91 96ABD0E7 CC365520 3F80927A
        1228D075 D434951A 9C678664 7D3AB62A 2B297263 82D92BA4
        36FFBFB0 A0A3FF7C A9932281 C183144E 631856A8 3BBE7588
        ACF1F6E5 1A4B1E76 480BC60C 5551EBC4 B6916580 4DB5AD25
        A5D7E9A5 BF184492 FB9EA6A7 479D586B 44F786BD 8A4F0228

Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB72 9216428C AAB82B22 AC7C3B0A
        F6149001 A1AE5EEA A5B08ABE D40B0946 203F5156 8BBA3866

Z is
        05756A96 5EC4FDDD D076DAD2 B6A4EEAC 7A72AB5A 5D0F9BB1
        8F9DFCF3 DB3F8DD4 02730BB4 7AC00C6C F40BC468 8FBD1EE1
        2B7B83A7 CB163C29 58BBAB27 C69D3F75 6F7BA8AE 7B0EA618

OtherInfo is

```
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         A31D24C8 BDADF88E 9499D594 FEB5A945
        11A03B91 96ABD0E7 CC365520 3F80927A 1228D075 D434951A
        9C678664 7D3AB62A 2B297263 82D92BA4 36FFBFB0 A0A3FF7C
        A9932281 C183144E 631856A8 3BBE7588 ACF1F6E5 1A4B1E76
        480BC60C 5551EBC4 B6916580 4DB5AD25 A5D7E9A5 BF184492
        FB9EA6A7 479D586B 44F786BD 8A4F0228 42A9C9B2 34D0677A
        46552B76 95A8F93A 090A5161 052645AC 30E19FFC 26A5A3F3


MacData is
                         4B435F31 5F55414C 49434542 4F424259
        0669AE9D 0C657ED8 5B6174DD FC33F02E 2A28B422 5A0BE50B
        DB8303E1 CFCEFFCC F113D6FA 07EEA236 E0E72BDE F678D424
        28CC0379 85DE19D4 E3BAF9A7 0B793CCD 0BC8E2EF E1AF5993
        00D54789 9C67ED17 B5F8997E 0D119729 2D06062A 8E7E7459
        CE620B0A C3F633BD 4A8AF428 59A1B0F9 53193CA3 062D310D
        9620B72C CD1B0A68 B34E9DA0 AD18BA34 48140686 8A2A57F5
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB72 9216428C AAB82B22 AC7C3B0A
        F6149001 A1AE5EEA A5B08ABE D40B0946 203F5156 8BBA3866


MacKey is
                                                 A31D24C8 BDADF88E
        9499D594 FEB5A945 11A03B91 96ABD0E7 CC365520 3F80927A


Mtag is
                         FB4E9D6D 78D0D2F7 DCC847A6 CC9FA1A5
        C98CCB86 6435692D 6D4BF1D1 327BB432 F56720C9 1041BE7C
        B4AB7B70 0E45307A 72FC3A07 B093DB4B 9B67BBBB 7F47800D


KeyData is
                                                 1228D075 D434951A
        9C678664 7D3AB62A 2B297263 82D92BA4 36FFBFB0 A0A3FF7C
        A9932281 C183144E 631856A8 3BBE7588 ACF1F6E5 1A4B1E76
        480BC60C 5551EBC4 B6916580 4DB5AD25 A5D7E9A5 BF184492
        FB9EA6A7 479D586B 44F786BD 8A4F0228 42A9C9B2 34D0677A
        46552B76 95A8F93A 090A5161 052645AC 30E19FFC 26A5A3F3
```

```
-----------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB72 9216428C AAB82B22 AC7C3B0A
        F6149001 A1AE5EEA A5B08ABE D40B0946 203F5156 8BBA3866


Z is
        05756A96 5EC4FDDD D076DAD2 B6A4EEAC 7A72AB5A 5D0F9BB1
        8F9DFCF3 DB3F8DD4 02730BB4 7AC00C6C F40BC468 8FBD1EE1
        2B7B83A7 CB163C29 58BBAB27 C69D3F75 6F7BA8AE 7B0EA618


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         A31D24C8 BDADF88E 9499D594 FEB5A945
        11A03B91 96ABD0E7 CC365520 3F80927A 1228D075 D434951A
        9C678664 7D3AB62A 2B297263 82D92BA4 36FFBFB0 A0A3FF7C
        A9932281 C183144E 631856A8 3BBE7588 ACF1F6E5 1A4B1E76
        480BC60C 5551EBC4 B6916580 4DB5AD25 A5D7E9A5 BF184492
        FB9EA6A7 479D586B 44F786BD 8A4F0228 42A9C9B2 34D0677A
        46552B76 95A8F93A 090A5161 052645AC 30E19FFC 26A5A3F3


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        0669AE9D 0C657ED8 5B6174DD FC33F02E 2A28B422 5A0BE50B
        DB8303E1 CFCEFFCC F113D6FA 07EEA236 E0E72BDE F678D424
        28CC0379 85DE19D4 E3BAF9A7 0B793CCD 0BC8E2EF E1AF5993
        00D54789 9C67ED17 B5F8997E 0D119729 2D06062A 8E7E7459
        CE620B0A C3F633BD 4A8AF428 59A1B0F9 53193CA3 062D310D
        9620B72C CD1B0A68 B34E9DA0 AD18BA34 48140686 8A2A57F5


MacKey is
                                             A31D24C8 BDADF88E
        9499D594 FEB5A945 11A03B91 96ABD0E7 CC365520 3F80927A


Mtag is
```

```
                        9B0145BF 01062605 B632DC27 A83947BD
        5AE4514D 7EA8C7E5 DA89877C 65507AB3 0BA65F06 BB049E47
        16BBC6BE D3A99BB1 28714805 9363B1B6 BDF4F21B 701337BD


KeyData is
                                                1228D075 D434951A
        9C678664 7D3AB62A 2B297263 82D92BA4 36FFBFB0 A0A3FF7C
        A9932281 C183144E 631856A8 3BBE7588 ACF1F6E5 1A4B1E76
        480BC60C 5551EBC4 B6916580 4DB5AD25 A5D7E9A5 BF184492
        FB9EA6A7 479D586B 44F786BD 8A4F0228 42A9C9B2 34D0677A
        46552B76 95A8F93A 090A5161 052645AC 30E19FFC 26A5A3F3




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB72 9216428C AAB82B22 AC7C3B0A
        F6149001 A1AE5EEA A5B08ABE D40B0946 203F5156 8BBA3866


Z is
        05756A96 5EC4FDDD D076DAD2 B6A4EEAC 7A72AB5A 5D0F9BB1
        8F9DFCF3 DB3F8DD4 02730BB4 7AC00C6C F40BC468 8FBD1EE1
        2B7B83A7 CB163C29 58BBAB27 C69D3F75 6F7BA8AE 7B0EA618


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                        A31D24C8 BDADF88E 9499D594 FEB5A945
        11A03B91 96ABD0E7 CC365520 3F80927A 1228D075 D434951A
        9C678664 7D3AB62A 2B297263 82D92BA4 36FFBFB0 A0A3FF7C
        A9932281 C183144E 631856A8 3BBE7588 ACF1F6E5 1A4B1E76
        480BC60C 5551EBC4 B6916580 4DB5AD25 A5D7E9A5 BF184492
        FB9EA6A7 479D586B 44F786BD 8A4F0228 42A9C9B2 34D0677A
        46552B76 95A8F93A 090A5161 052645AC 30E19FFC 26A5A3F3


U2V
----------------
```

```
MacData is
                        4B435F32 5F55414C 49434542 4F424259
        0669AE9D 0C657ED8 5B6174DD FC33F02E 2A28B422 5A0BE50B
        DB8303E1 CFCEFFCC F113D6FA 07EEA236 E0E72BDE F678D424
        28CC0379 85DE19D4 E3BAF9A7 0B793CCD 0BC8E2EF E1AF5993
        00D54789 9C67ED17 B5F8997E 0D119729 2D06062A 8E7E7459
        CE620B0A C3F633BD 4A8AF428 59A1B0F9 53193CA3 062D310D
        9620B72C CD1B0A68 B34E9DA0 AD18BA34 48140686 8A2A57F5
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB72 9216428C AAB82B22 AC7C3B0A
        F6149001 A1AE5EEA A5B08ABE D40B0946 203F5156 8BBA3866


MacKey is
                                                A31D24C8 BDADF88E
        9499D594 FEB5A945 11A03B91 96ABD0E7 CC365520 3F80927A


Mtag is
                        645362A9 9DDD8441 C175DD24 29C6CDC0
        6B006FC6 A93C59E3 5984F5BD 4483BC14 F01BBBEE EC45990C
        E5BE9C8A 8CDBD6BF 3F43FD0A 114A8CA3 CFCC8432 2D1A4A74


V2U
----------------
MacData is
                        4B435F32 5F56424F 42425941 4C494345
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB72 9216428C AAB82B22 AC7C3B0A
        F6149001 A1AE5EEA A5B08ABE D40B0946 203F5156 8BBA3866
        0669AE9D 0C657ED8 5B6174DD FC33F02E 2A28B422 5A0BE50B
        DB8303E1 CFCEFFCC F113D6FA 07EEA236 E0E72BDE F678D424
        28CC0379 85DE19D4 E3BAF9A7 0B793CCD 0BC8E2EF E1AF5993
        00D54789 9C67ED17 B5F8997E 0D119729 2D06062A 8E7E7459
        CE620B0A C3F633BD 4A8AF428 59A1B0F9 53193CA3 062D310D
        9620B72C CD1B0A68 B34E9DA0 AD18BA34 48140686 8A2A57F5


MacKey is
                                                A31D24C8 BDADF88E
        9499D594 FEB5A945 11A03B91 96ABD0E7 CC365520 3F80927A


Mtag is
                        0BE17126 B588F9CA 9C569EC1 65E366C8
```

8398A442 1A256F36 0F0BE137 9F0C8883 B0BCF31F BA19DD74
35FF515B 6EB4FA42 D5D25D95 02E5C77B B7E35749 7C9BEE8C

KeyData is
1228D075 D434951A
9C678664 7D3AB62A 2B297263 82D92BA4 36FFBFB0 A0A3FF7C
A9932281 C183144E 631856A8 3BBE7588 ACF1F6E5 1A4B1E76
480BC60C 5551EBC4 B6916580 4DB5AD25 A5D7E9A5 BF184492
FB9EA6A7 479D586B 44F786BD 8A4F0228 42A9C9B2 34D0677A
46552B76 95A8F93A 090A5161 052645AC 30E19FFC 26A5A3F3

OnePassDiffieHellmanCDH(K-571)
---
dsV is
01823854 AF10876C 19AEE8EC 6691AD9E 7E294860 5347F7DF
0EB770FE EB2E71B9 8FAB326F FAEDFEE6 7093A304 8B79CA07
C7A718DD 32DE5305 48D0FD9B 553AFC00 0E927766 61F71FBB

QsV_x is
04C74E10 D370016A 080BEDD0 E852F986 EFC63CAC 08BF055C
795CD634 DF8BEB7A 4411AB19 358E58AC 8000F22F 9528F4E1
CBF128B6 B5871363 4D62415E BFCD5A5A 94653F8D FDF0703B

QsV_y is
06E73204 610FA3AC B35DD890 F03D2E5C 9BFA20DD 29DA26B6
4B13DEC6 399061A2 DB2BBB0B 6CCF848C 6567B5FA 220AB1B8
2A70DF20 F2B4105B DA8520C2 02BF828A 56A67DDC B9E79B24

deU is
013AC597 40DDBC84 E4803312 4D269467 71CC4872 706EF9F6
34CE0E8A F1A227E8 E14A088E 9B274ADD 07249E3B 8FC69719
10EDE19F 15F9CF94 6BF59829 1F372BD0 7CE0824B 40E5B486

QeU_x is
0669AE9D 0C657ED8 5B6174DD FC33F02E 2A28B422 5A0BE50B
DB8303E1 CFCEFFCC F113D6FA 07EEA236 E0E72BDE F678D424
28CC0379 85DE19D4 E3BAF9A7 0B793CCD 0BC8E2EF E1AF5993

```
QeU_y is
        00D54789 9C67ED17 B5F8997E 0D119729 2D06062A 8E7E7459
        CE620B0A C3F633BD 4A8AF428 59A1B0F9 53193CA3 062D310D
        9620B72C CD1B0A68 B34E9DA0 AD18BA34 48140686 8A2A57F5




------------------------------------------------------------
no Key Confirmation
Z is
        05F36BAF 06996B30 AF14EE01 E92CC6A7 2D15CFBA F32F22AC
        946C496D 46A89D95 93CB1872 6A087E7E 4268DBFE ABC0F806
        3A208335 11025BB7 47210411 D2EE1AC1 C89E68EA 566AAA37


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                            9885E160 651A3442
        20A987D4 8135BB2C D5DC1B9B AFA57AEC DEB61687 6E5A3696
        08D42C66 B81D5331 88721044 397E573A E9AFF610 D644BE32
        5C142FA2 A9917D90 A7B17222 B73C1C6A 80D629D9 B669E8B9
        DE0B7CBD 08157795 D7CCC7CD DCA0E465 3890E5A6 65C939CF
        E67E901B 4788A9C1 80AB142E 07C87797 F853CC87 6DD2A20D


KeyData is
                                            9885E160 651A3442
        20A987D4 8135BB2C D5DC1B9B AFA57AEC DEB61687 6E5A3696
        08D42C66 B81D5331 88721044 397E573A E9AFF610 D644BE32
        5C142FA2 A9917D90 A7B17222 B73C1C6A 80D629D9 B669E8B9
        DE0B7CBD 08157795 D7CCC7CD DCA0E465 3890E5A6 65C939CF
        E67E901B 4788A9C1 80AB142E 07C87797 F853CC87 6DD2A20D




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
        05F36BAF 06996B30 AF14EE01 E92CC6A7 2D15CFBA F32F22AC
        946C496D 46A89D95 93CB1872 6A087E7E 4268DBFE ABC0F806
```

```
        3A208335 11025BB7 47210411 D2EE1AC1 C89E68EA 566AAA37


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         9885E160 651A3442 20A987D4 8135BB2C
        D5DC1B9B AFA57AEC DEB61687 6E5A3696 08D42C66 B81D5331
        88721044 397E573A E9AFF610 D644BE32 5C142FA2 A9917D90
        A7B17222 B73C1C6A 80D629D9 B669E8B9 DE0B7CBD 08157795
        D7CCC7CD DCA0E465 3890E5A6 65C939CF E67E901B 4788A9C1
        80AB142E 07C87797 F853CC87 6DD2A20D A9F7E489 6A8E7A01
        5BA9650C FCAFDF1D 8655F155 9C3731D1 E6C8B0A9 8A184425


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        0669AE9D 0C657ED8 5B6174DD FC33F02E 2A28B422 5A0BE50B
        DB8303E1 CFCEFFCC F113D6FA 07EEA236 E0E72BDE F678D424
        28CC0379 85DE19D4 E3BAF9A7 0B793CCD 0BC8E2EF E1AF5993
        00D54789 9C67ED17 B5F8997E 0D119729 2D06062A 8E7E7459
        CE620B0A C3F633BD 4A8AF428 59A1B0F9 53193CA3 062D310D
        9620B72C CD1B0A68 B34E9DA0 AD18BA34 48140686 8A2A57F5


MacKey is
                                               9885E160 651A3442
        20A987D4 8135BB2C D5DC1B9B AFA57AEC DEB61687 6E5A3696


Mtag is
                         50EA9AFC 940A0DFA 3A7DF1EC A6B66815
        E899CE6F 65D3360A D6F5907F 712A2F9E CD51715D FA5D8FB2
        04759DE4 5AC472A8 84EAB091 6F7A5F68 259D4A71 F8A7F5E6


KeyData is
                                               08D42C66 B81D5331
        88721044 397E573A E9AFF610 D644BE32 5C142FA2 A9917D90
        A7B17222 B73C1C6A 80D629D9 B669E8B9 DE0B7CBD 08157795
        D7CCC7CD DCA0E465 3890E5A6 65C939CF E67E901B 4788A9C1
        80AB142E 07C87797 F853CC87 6DD2A20D A9F7E489 6A8E7A01
        5BA9650C FCAFDF1D 8655F155 9C3731D1 E6C8B0A9 8A184425
```

StaticUnifiedCDH(K-571)
---
dsU is
009B592D 32F99420 05A38021 D26E7AA6 ED3E78BB DFF2A861
311B89C9 9DF67762 8EE47F3D BFD26F35 5518F493 35B09D0A
E89DFA20 C5FE7724 DE0C49CB 0CBD53A1 9E19CE35 DB00978C

QsU_x is
03F19CFE 63178885 1373B8C4 44CA6515 2F33AF3B B7904D91
FDAC9ACE B649AA9E 0F10AD6D 40A6511F 78DD7408 40E09541
B2CF4211 75B126B0 6E3EFD1F 66AC0D53 8F88E03D 2FC566E9

QsU_y is
0090E2D3 8D4052FC 89E19F52 A948B01F 19C8BE26 64ACC69C
491964EA 1CC9B66F A3797CBD 0EA82707 6195DFFD 1B49B1A0
5CAE1068 2A002139 B9499FEF 8A8EAA35 1DC36921 C768BA81

dsV is
01823854 AF10876C 19AEE8EC 6691AD9E 7E294860 5347F7DF
0EB770FE EB2E71B9 8FAB3270 3EF2071A 90AC630C 8F9BFE0B
D86718E5 3EE255FE B95F039C F54D0400 31AF98BE BEFB1FFB

QsV_x is
05DB1E98 F63C153E 85D418A0 BDB68114 F78C4F6B 93F98312
F663BE3A B6E4F851 F19B8092 32738EE2 7589D84E BC26D260
75E97D08 136B4621 0B7B29DA 98410795 CE72D468 5BE4CF2D

QsV_y is
01585B12 EBB40461 066DE01A 6131D8A7 32DCAC9A 2068B65E
F3118574 BC4C518D A597D411 FADD99F7 ED2092D0 A95819D3
92A6D58F C38305AC 43AE296A CCDAF1A9 777DD08F A05AB625

---
no Key Confirmation
NonceU is

```
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB72 9216428C AAB82B22 AC7C3B0A
        F6149001 A1AE5EEA A5B08ABE D40B0946 203F5156 8BBA3866


Z is
        04230AA5 9F3565C9 62F274E5 3DD6BFE5 9D70B9CD 0482F0DF
        88D97AB4 4D031A65 24917A12 B8DA2DF8 E1D55094 49D4D0E1
        08D19490 0DA5D5BF 95CA6BA5 562A406D E876366C AFE75E9D


OtherInfo is
                                                            1234
        56789ABC DEF0414C 49434531 32333B02 0051D0BA 0638CE20
        905F7F3A 0298275E 33482000 1D90F0B2 F19737D1 F8452AC5
        54BEEB72 9216428C AAB82B22 AC7C3B0A F6149001 A1AE5EEA
        A5B08ABE D40B0946 203F5156 8BBA3866 424F4242 59343536


DerivedKeyMaterial is
                                            170F9696 B945EEF8
        5D01DC2A B9AAF9FC 6F1BB0FC 99C76D10 6955B119 49385CBC
        70ECF6C4 BC0512CB E3097C73 C21D5784 886481AC 90126AB2
        64B7AE65 5ABB452D 164048C9 A26BF8BD DE3417BE 94567807
        CE8CE6A1 E2635C44 B4C2C084 5E19D020 DC0B7375 9BB009D3
        6DDD6AAD EF18E138 4872FA59 8A69B847 77740286 C19CF85C


KeyData is
                                            170F9696 B945EEF8
        5D01DC2A B9AAF9FC 6F1BB0FC 99C76D10 6955B119 49385CBC
        70ECF6C4 BC0512CB E3097C73 C21D5784 886481AC 90126AB2
        64B7AE65 5ABB452D 164048C9 A26BF8BD DE3417BE 94567807
        CE8CE6A1 E2635C44 B4C2C084 5E19D020 DC0B7375 9BB009D3
        6DDD6AAD EF18E138 4872FA59 8A69B847 77740286 C19CF85C




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceU is
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB72 9216428C AAB82B22 AC7C3B0A
        F6149001 A1AE5EEA A5B08ABE D40B0946 203F5156 8BBA3866
```

NonceV is
        00A05A4D DA59C82A 26EAF7F8 44D4C41E 622F4AA9 17AB5F06
        5A452352 1700C41A 5234B393 15098335 8FD81684 23D203D2
        473DF4D6 EA01134E 6F415BCD 2702CA3F A4548D45 34B4294B

Z is
        04230AA5 9F3565C9 62F274E5 3DD6BFE5 9D70B9CD 0482F0DF
        88D97AB4 4D031A65 24917A12 B8DA2DF8 E1D55094 49D4D0E1
        08D19490 0DA5D5BF 95CA6BA5 562A406D E876366C AFE75E9D

OtherInfo is
                                                            1234
        56789ABC DEF0414C 49434531 32333B02 0051D0BA 0638CE20
        905F7F3A 0298275E 33482000 1D90F0B2 F19737D1 F8452AC5
        54BEEB72 9216428C AAB82B22 AC7C3B0A F6149001 A1AE5EEA
        A5B08ABE D40B0946 203F5156 8BBA3866 424F4242 59343536

DerivedKeyMaterial is
                           170F9696 B945EEF8 5D01DC2A B9AAF9FC
        6F1BB0FC 99C76D10 6955B119 49385CBC 70ECF6C4 BC0512CB
        E3097C73 C21D5784 886481AC 90126AB2 64B7AE65 5ABB452D
        164048C9 A26BF8BD DE3417BE 94567807 CE8CE6A1 E2635C44
        B4C2C084 5E19D020 DC0B7375 9BB009D3 6DDD6AAD EF18E138
        4872FA59 8A69B847 77740286 C19CF85C 737D257F 27420B8D
        430C7FE5 4C8382A9 531CCFCD 4B146465 935EE8C1 ECF28058

MacData is
                           4B435F31 5F55414C 49434542 4F424259
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB72 9216428C AAB82B22 AC7C3B0A
        F6149001 A1AE5EEA A5B08ABE D40B0946 203F5156 8BBA3866
        00A05A4D DA59C82A 26EAF7F8 44D4C41E 622F4AA9 17AB5F06
        5A452352 1700C41A 5234B393 15098335 8FD81684 23D203D2
        473DF4D6 EA01134E 6F415BCD 2702CA3F A4548D45 34B4294B

MacKey is
                                                 170F9696 B945EEF8
        5D01DC2A B9AAF9FC 6F1BB0FC 99C76D10 6955B119 49385CBC

Mtag is
                        8CDBC651 C97ABB36 D2E7EA21 60CC1C82
        FBEF47E8 C1616705 53544CA4 6029C882 BF0DC3FC 4514357F
        33794BE2 A47066FF B01B98A9 7E9B1EE8 C55EB4DD 5A89AF8A

KeyData is
                                                70ECF6C4 BC0512CB
        E3097C73 C21D5784 886481AC 90126AB2 64B7AE65 5ABB452D
        164048C9 A26BF8BD DE3417BE 94567807 CE8CE6A1 E2635C44
        B4C2C084 5E19D020 DC0B7375 9BB009D3 6DDD6AAD EF18E138
        4872FA59 8A69B847 77740286 C19CF85C 737D257F 27420B8D
        430C7FE5 4C8382A9 531CCFCD 4B146465 935EE8C1 ECF28058

Scheme Responder, Key Confirmation Provider: V to U
NonceV is
        00A05A4D DA59C82A 26EAF7F8 44D4C41E 622F4AA9 17AB5F06
        5A452352 1700C41A 5234B393 15098335 8FD81684 23D203D2
        473DF4D6 EA01134E 6F415BCD 2702CA3F A4548D45 34B4294B

NonceU is
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB72 9216428C AAB82B22 AC7C3B0A
        F6149001 A1AE5EEA A5B08ABE D40B0946 203F5156 8BBA3866

Z is
        04230AA5 9F3565C9 62F274E5 3DD6BFE5 9D70B9CD 0482F0DF
        88D97AB4 4D031A65 24917A12 B8DA2DF8 E1D55094 49D4D0E1
        08D19490 0DA5D5BF 95CA6BA5 562A406D E876366C AFE75E9D

OtherInfo is
                                                            1234
        56789ABC DEF0414C 49434531 32333B02 0051D0BA 0638CE20
        905F7F3A 0298275E 33482000 1D90F0B2 F19737D1 F8452AC5
        54BEEB72 9216428C AAB82B22 AC7C3B0A F6149001 A1AE5EEA
        A5B08ABE D40B0946 203F5156 8BBA3866 424F4242 59343536

DerivedKeyMaterial is

```
                        170F9696 B945EEF8 5D01DC2A B9AAF9FC
        6F1BB0FC 99C76D10 6955B119 49385CBC 70ECF6C4 BC0512CB
        E3097C73 C21D5784 886481AC 90126AB2 64B7AE65 5ABB452D
        164048C9 A26BF8BD DE3417BE 94567807 CE8CE6A1 E2635C44
        B4C2C084 5E19D020 DC0B7375 9BB009D3 6DDD6AAD EF18E138
        4872FA59 8A69B847 77740286 C19CF85C 737D257F 27420B8D
        430C7FE5 4C8382A9 531CCFCD 4B146465 935EE8C1 ECF28058


MacData is
                        4B435F31 5F56424F 42425941 4C494345
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB72 9216428C AAB82B22 AC7C3B0A
        F6149001 A1AE5EEA A5B08ABE D40B0946 203F5156 8BBA3866


MacKey is
                                              170F9696 B945EEF8
        5D01DC2A B9AAF9FC 6F1BB0FC 99C76D10 6955B119 49385CBC


Mtag is
                        B3BD763B 63030ACD 8402824D 318D8E21
        AB7DAEEE 75FEFF87 A08E3FCE 3833713F 19914623 F05FF4B6
        E11F0F24 E86765F3 9473A098 75DD90DF E2CD48E2 A23B961B


KeyData is
                                              70ECF6C4 BC0512CB
        E3097C73 C21D5784 886481AC 90126AB2 64B7AE65 5ABB452D
        164048C9 A26BF8BD DE3417BE 94567807 CE8CE6A1 E2635C44
        B4C2C084 5E19D020 DC0B7375 9BB009D3 6DDD6AAD EF18E138
        4872FA59 8A69B847 77740286 C19CF85C 737D257F 27420B8D
        430C7FE5 4C8382A9 531CCFCD 4B146465 935EE8C1 ECF28058




-------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
NonceU is
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB72 9216428C AAB82B22 AC7C3B0A
        F6149001 A1AE5EEA A5B08ABE D40B0946 203F5156 8BBA3866
```

```
NonceV is
        00A05A4D DA59C82A 26EAF7F8 44D4C41E 622F4AA9 17AB5F06
        5A452352 1700C41A 5234B393 15098335 8FD81684 23D203D2
        473DF4D6 EA01134E 6F415BCD 2702CA3F A4548D45 34B4294B


Z is
        04230AA5 9F3565C9 62F274E5 3DD6BFE5 9D70B9CD 0482F0DF
        88D97AB4 4D031A65 24917A12 B8DA2DF8 E1D55094 49D4D0E1
        08D19490 0DA5D5BF 95CA6BA5 562A406D E876366C AFE75E9D


OtherInfo is
                                                          1234
        56789ABC DEF0414C 49434531 32333B02 0051D0BA 0638CE20
        905F7F3A 0298275E 33482000 1D90F0B2 F19737D1 F8452AC5
        54BEEB72 9216428C AAB82B22 AC7C3B0A F6149001 A1AE5EEA
        A5B08ABE D40B0946 203F5156 8BBA3866 424F4242 59343536


DerivedKeyMaterial is
                          170F9696 B945EEF8 5D01DC2A B9AAF9FC
        6F1BB0FC 99C76D10 6955B119 49385CBC 70ECF6C4 BC0512CB
        E3097C73 C21D5784 886481AC 90126AB2 64B7AE65 5ABB452D
        164048C9 A26BF8BD DE3417BE 94567807 CE8CE6A1 E2635C44
        B4C2C084 5E19D020 DC0B7375 9BB009D3 6DDD6AAD EF18E138
        4872FA59 8A69B847 77740286 C19CF85C 737D257F 27420B8D
        430C7FE5 4C8382A9 531CCFCD 4B146465 935EE8C1 ECF28058


U2V
----------------
MacData is
                          4B435F32 5F55414C 49434542 4F424259
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB72 9216428C AAB82B22 AC7C3B0A
        F6149001 A1AE5EEA A5B08ABE D40B0946 203F5156 8BBA3866
        00A05A4D DA59C82A 26EAF7F8 44D4C41E 622F4AA9 17AB5F06
        5A452352 1700C41A 5234B393 15098335 8FD81684 23D203D2
        473DF4D6 EA01134E 6F415BCD 2702CA3F A4548D45 34B4294B


MacKey is
                                                  170F9696 B945EEF8
        5D01DC2A B9AAF9FC 6F1BB0FC 99C76D10 6955B119 49385CBC
```

```
Mtag is
                        23608B95 FE044F7E 37DEB733 36A00AE4
        587828CC 56565614 0F0C0F35 56996AB5 84527820 45C87054
        394F4A7F 7BE9F716 8537EEB3 D6CDFD8B ADA3F5B7 A7FED463


V2U
----------------
MacData is
                        4B435F32 5F56424F 42425941 4C494345
        00A05A4D DA59C82A 26EAF7F8 44D4C41E 622F4AA9 17AB5F06
        5A452352 1700C41A 5234B393 15098335 8FD81684 23D203D2
        473DF4D6 EA01134E 6F415BCD 2702CA3F A4548D45 34B4294B
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB72 9216428C AAB82B22 AC7C3B0A
        F6149001 A1AE5EEA A5B08ABE D40B0946 203F5156 8BBA3866


MacKey is
                                                170F9696 B945EEF8
        5D01DC2A B9AAF9FC 6F1BB0FC 99C76D10 6955B119 49385CBC


Mtag is
                        5929EB11 C7186DEA F4EC9A26 735157F2
        BCAE19A3 CABFE403 BF957236 22C90C5D 869780FC 080987B0
        DE9099CD 15171B4E EFBCE317 813D8CB7 CEC6030A 67DDEFB9


KeyData is
                                                70ECF6C4 BC0512CB
        E3097C73 C21D5784 886481AC 90126AB2 64B7AE65 5ABB452D
        164048C9 A26BF8BD DE3417BE 94567807 CE8CE6A1 E2635C44
        B4C2C084 5E19D020 DC0B7375 9BB009D3 6DDD6AAD EF18E138
        4872FA59 8A69B847 77740286 C19CF85C 737D257F 27420B8D
        430C7FE5 4C8382A9 531CCFCD 4B146465 935EE8C1 ECF28058
```

FullUnifiedCDH(B-571)
---
dsU is
009B592D 32F99420 05A38021 D26E7AA6 ED3E78BB DFF2A861
311B89C9 9DF67762 8EE47F41 AE6A231F 90B13028 98478B30
FB2F883C 29CD681D 376A9FA6 7AE2FAEB FC7A4B59 440D84F7

QsU_x is
04B1D9CD E0F54AAC 99E02B4A B0B0705C 2CAF033B C44C1304
04066DCA DA8E0783 24CBADEE 20B23C91 46F3B0CC 60CD947D
AD7AA111 C7269CBB FBB6B776 B5F61433 C8F5451B 0E221457

QsU_y is
0050459A AA86CD0B B4260071 9DBB9505 A6FE6CED 59CFC1A7
4104845C EC957A88 D15A53C9 2DF39B52 B0060082 BD9B3203
DBE10B82 0B77BBFA 5694AB23 E33FFC56 5831F5BC 1E479199

dsV is
01823854 AF10876C 19AEE8EC 6691AD9E 7E294860 5347F7DF
0EB770FE EB2E71B9 8FAB3273 F7DB3994 AE86986A 7D5533F3
7556EE07 7B1F9270 A1B990CA 10296BA3 7632CD9F D2F43B6B

QsV_x is
0431E29F 977CDEA2 90E063C8 3F6B4A0D E33D083C C1844BC4
60303F63 53FB2B86 888C1BA7 81F89A6E FFA2447C F1E4E772
E77E8FF6 3243DE77 1692EB0B AE333456 8CF11AE0 9422916F

QsV_y is
01530D05 C336B8C0 121149A2 3416951E D557A58E 4F2A6F64
3CFBA1F1 D508C329 100302D2 BB783676 E0AECE33 EBA2FBFC
8057E158 D9447DC6 D6BF523D 3077CAB6 9590871E C80155B1

deU is
013AC597 40DDBC84 E4803312 4D269467 71CC4872 706EF9F6
34CE0E8A F1A227E8 E14A0898 53A989E5 BE24D464 0D4D6947
884A7936 2618DA2A 14AC7EEB 06DC5BEE C9775477 444EA803

QeU_x is
077192C3 24FDDF48 74D8B788 244F004F 30FD9A85 9CDB919E
97CFAE95 16A2703B 56B1EDB8 8D53C17E 3F1A0F4B AF21DA3B
8ED082BD FE53ACEF F6BB4DE6 93DD4209 DD2D1289 1B594C4C

QeU_y is
05D56CA3 56C46D67 2E8A73CD D02164B7 7A3C54CC 1306B270
00C70545 3F56BB41 4B191BA3 AE3E2FC1 85AFF2A7 873354DE
60A21538 039460C3 82456E4C 04FECE44 289F1DFD FE6FB4DE

deV is
0035076B C0FAE543 F8E32E41 3BD442A5 4EF489B8 9927B021
0360F83F 8703C448 C72F4558 9051B18E B65E1FAE 250BBFEA
6DC924B8 DCD4893F 66DFC547 2479B3AB ADA7E32B C6EF6672

QeV_x is
024DB1B7 735FD38B 790E3417 BDFD156B 2F540F89 183B35D1
3A982827 7D9B0C8D D99C3261 07E8F8A1 27EC70BC ACA0C8AB
D59D5A15 0BF8C0CF 81C82DDE FC29B90C E6A65890 9C37AE00

QeV_y is
0067E1B3 45827EA0 A4E45CB7 2367C8E5 260A8680 6DFED31C
C7DAEC9A 794AA6D4 C1680494 29CAFD82 70C498DF 411B4888
8244268D 9F1D5F6F 494BD092 8ABDB1EF DD3D6E3D FA2F8305

---

no Key Confirmation
Zs is
07060501 2021D902 A25C59CA D8D2DFA1 4545C6C6 5A45B26B
8F3D3812 84F10213 58859BA3 2E0B9666 A72AFF29 7A14203B
FB630E2F FAA896C2 34A04802 B4862806 07F2B1DD 4013A201

Ze is
03E43CE9 090F3AC6 3B6FB8AE CF99371F 00F3B053 7CF96D44
7B10A595 CC60EC48 74F476CE 60175602 3AB93E07 53A049B6
45708A21 F2322D47 ACF1E2EC AD9731CA 7B7335F4 AB1B03B8

Z is
        03E43CE9 090F3AC6 3B6FB8AE CF99371F 00F3B053 7CF96D44
        7B10A595 CC60EC48 74F476CE 60175602 3AB93E07 53A049B6
        45708A21 F2322D47 ACF1E2EC AD9731CA 7B7335F4 AB1B03B8
        07060501 2021D902 A25C59CA D8D2DFA1 4545C6C6 5A45B26B
        8F3D3812 84F10213 58859BA3 2E0B9666 A72AFF29 7A14203B
        FB630E2F FAA896C2 34A04802 B4862806 07F2B1DD 4013A201

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                                            180ECF36 89813BC5
        397C86FD A3419BF3 2922F048 88FD9B29 7CB0FADA 7EF5E180
        762DFEB8 91B1AAC6 93D04E7F 7272D5C1 8CF96111 C894D3E3
        A03AFC7B 6A88F1CF CEEB9DF7 024A872C A35B1FA7 C9E95D34
        05572484 3054B600 20AA2E00 80E9FB2B CEAC66B4 68D7E218
        93265CB6 770C8890 02117294 B818273B B6E8CAF1 119FE4C7

KeyData is
                                            180ECF36 89813BC5
        397C86FD A3419BF3 2922F048 88FD9B29 7CB0FADA 7EF5E180
        762DFEB8 91B1AAC6 93D04E7F 7272D5C1 8CF96111 C894D3E3
        A03AFC7B 6A88F1CF CEEB9DF7 024A872C A35B1FA7 C9E95D34
        05572484 3054B600 20AA2E00 80E9FB2B CEAC66B4 68D7E218
        93265CB6 770C8890 02117294 B818273B B6E8CAF1 119FE4C7

Scheme Initiator, Key Confirmation Provider: U to V
Zs is
        07060501 2021D902 A25C59CA D8D2DFA1 4545C6C6 5A45B26B
        8F3D3812 84F10213 58859BA3 2E0B9666 A72AFF29 7A14203B
        FB630E2F FAA896C2 34A04802 B4862806 07F2B1DD 4013A201

Ze is
        03E43CE9 090F3AC6 3B6FB8AE CF99371F 00F3B053 7CF96D44
        7B10A595 CC60EC48 74F476CE 60175602 3AB93E07 53A049B6
        45708A21 F2322D47 ACF1E2EC AD9731CA 7B7335F4 AB1B03B8

Z is
        03E43CE9 090F3AC6 3B6FB8AE CF99371F 00F3B053 7CF96D44
        7B10A595 CC60EC48 74F476CE 60175602 3AB93E07 53A049B6
        45708A21 F2322D47 ACF1E2EC AD9731CA 7B7335F4 AB1B03B8
        07060501 2021D902 A25C59CA D8D2DFA1 4545C6C6 5A45B26B
        8F3D3812 84F10213 58859BA3 2E0B9666 A72AFF29 7A14203B
        FB630E2F FAA896C2 34A04802 B4862806 07F2B1DD 4013A201

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                         180ECF36 89813BC5 397C86FD A3419BF3
        2922F048 88FD9B29 7CB0FADA 7EF5E180 762DFEB8 91B1AAC6
        93D04E7F 7272D5C1 8CF96111 C894D3E3 A03AFC7B 6A88F1CF
        CEEB9DF7 024A872C A35B1FA7 C9E95D34 05572484 3054B600
        20AA2E00 80E9FB2B CEAC66B4 68D7E218 93265CB6 770C8890
        02117294 B818273B B6E8CAF1 119FE4C7 8A00C2C0 EAFD66F3
        5581F0EB A040FD2B C3751560 935B2874 FC8D18D5 5FF71FFC

MacData is
                         4B435F31 5F55414C 49434542 4F424259
        077192C3 24FDDF48 74D8B788 244F004F 30FD9A85 9CDB919E
        97CFAE95 16A2703B 56B1EDB8 8D53C17E 3F1A0F4B AF21DA3B
        8ED082BD FE53ACEF F6BB4DE6 93DD4209 DD2D1289 1B594C4C
        05D56CA3 56C46D67 2E8A73CD D02164B7 7A3C54CC 1306B270
        00C70545 3F56BB41 4B191BA3 AE3E2FC1 85AFF2A7 873354DE
        60A21538 039460C3 82456E4C 04FECE44 289F1DFD FE6FB4DE
        024DB1B7 735FD38B 790E3417 BDFD156B 2F540F89 183B35D1
        3A982827 7D9B0C8D D99C3261 07E8F8A1 27EC70BC ACA0C8AB
        D59D5A15 0BF8C0CF 81C82DDE FC29B90C E6A65890 9C37AE00
        0067E1B3 45827EA0 A4E45CB7 2367C8E5 260A8680 6DFED31C
        C7DAEC9A 794AA6D4 C1680494 29CAFD82 70C498DF 411B4888
        8244268D 9F1D5F6F 494BD092 8ABDB1EF DD3D6E3D FA2F8305

MacKey is
                                                 180ECF36 89813BC5
        397C86FD A3419BF3 2922F048 88FD9B29 7CB0FADA 7EF5E180

Mtag is

```
                        31CF6C71 FE86FE2C 644E9608 736DC70E
        E2CAC02C 7F64B3B9 5B17B2B4 6F1F80C7 25C5749B 535C20D0
        F4233EA7 91AD478E B6DFF0D4 B1310999 73C5B8C6 DFCDE601


KeyData is
                                                762DFEB8 91B1AAC6
        93D04E7F 7272D5C1 8CF96111 C894D3E3 A03AFC7B 6A88F1CF
        CEEB9DF7 024A872C A35B1FA7 C9E95D34 05572484 3054B600
        20AA2E00 80E9FB2B CEAC66B4 68D7E218 93265CB6 770C8890
        02117294 B818273B B6E8CAF1 119FE4C7 8A00C2C0 EAFD66F3
        5581F0EB A040FD2B C3751560 935B2874 FC8D18D5 5FF71FFC




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Zs is
        07060501 2021D902 A25C59CA D8D2DFA1 4545C6C6 5A45B26B
        8F3D3812 84F10213 58859BA3 2E0B9666 A72AFF29 7A14203B
        FB630E2F FAA896C2 34A04802 B4862806 07F2B1DD 4013A201


Ze is
        03E43CE9 090F3AC6 3B6FB8AE CF99371F 00F3B053 7CF96D44
        7B10A595 CC60EC48 74F476CE 60175602 3AB93E07 53A049B6
        45708A21 F2322D47 ACF1E2EC AD9731CA 7B7335F4 AB1B03B8


Z is
        03E43CE9 090F3AC6 3B6FB8AE CF99371F 00F3B053 7CF96D44
        7B10A595 CC60EC48 74F476CE 60175602 3AB93E07 53A049B6
        45708A21 F2322D47 ACF1E2EC AD9731CA 7B7335F4 AB1B03B8
        07060501 2021D902 A25C59CA D8D2DFA1 4545C6C6 5A45B26B
        8F3D3812 84F10213 58859BA3 2E0B9666 A72AFF29 7A14203B
        FB630E2F FAA896C2 34A04802 B4862806 07F2B1DD 4013A201


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                        180ECF36 89813BC5 397C86FD A3419BF3
        2922F048 88FD9B29 7CB0FADA 7EF5E180 762DFEB8 91B1AAC6
```

```
        93D04E7F 7272D5C1 8CF96111 C894D3E3 A03AFC7B 6A88F1CF
        CEEB9DF7 024A872C A35B1FA7 C9E95D34 05572484 3054B600
        20AA2E00 80E9FB2B CEAC66B4 68D7E218 93265CB6 770C8890
        02117294 B818273B B6E8CAF1 119FE4C7 8A00C2C0 EAFD66F3
        5581F0EB A040FD2B C3751560 935B2874 FC8D18D5 5FF71FFC


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        024DB1B7 735FD38B 790E3417 BDFD156B 2F540F89 183B35D1
        3A982827 7D9B0C8D D99C3261 07E8F8A1 27EC70BC ACA0C8AB
        D59D5A15 0BF8C0CF 81C82DDE FC29B90C E6A65890 9C37AE00
        0067E1B3 45827EA0 A4E45CB7 2367C8E5 260A8680 6DFED31C
        C7DAEC9A 794AA6D4 C1680494 29CAFD82 70C498DF 411B4888
        8244268D 9F1D5F6F 494BD092 8ABDB1EF DD3D6E3D FA2F8305
        077192C3 24FDDF48 74D8B788 244F004F 30FD9A85 9CDB919E
        97CFAE95 16A2703B 56B1EDB8 8D53C17E 3F1A0F4B AF21DA3B
        8ED082BD FE53ACEF F6BB4DE6 93DD4209 DD2D1289 1B594C4C
        05D56CA3 56C46D67 2E8A73CD D02164B7 7A3C54CC 1306B270
        00C70545 3F56BB41 4B191BA3 AE3E2FC1 85AFF2A7 873354DE
        60A21538 039460C3 82456E4C 04FECE44 289F1DFD FE6FB4DE


MacKey is
                                                 180ECF36 89813BC5
        397C86FD A3419BF3 2922F048 88FD9B29 7CB0FADA 7EF5E180


Mtag is
                         F533517F 35348185 92D1A139 B395610A
        A89C52EC 23D49CF5 D9E26D01 C3E92CD1 556DB33B CBAA5234
        6EC14944 B846291C 1DE8DDFF 5F730EB2 61CCFCA1 FF546565


KeyData is
                                                 762DFEB8 91B1AAC6
        93D04E7F 7272D5C1 8CF96111 C894D3E3 A03AFC7B 6A88F1CF
        CEEB9DF7 024A872C A35B1FA7 C9E95D34 05572484 3054B600
        20AA2E00 80E9FB2B CEAC66B4 68D7E218 93265CB6 770C8890
        02117294 B818273B B6E8CAF1 119FE4C7 8A00C2C0 EAFD66F3
        5581F0EB A040FD2B C3751560 935B2874 FC8D18D5 5FF71FFC



-------------------------------------------------------------
```

```
Scheme Initiator, Key Confirmation Bilateral
Zs is
        07060501 2021D902 A25C59CA D8D2DFA1 4545C6C6 5A45B26B
        8F3D3812 84F10213 58859BA3 2E0B9666 A72AFF29 7A14203B
        FB630E2F FAA896C2 34A04802 B4862806 07F2B1DD 4013A201


Ze is
        03E43CE9 090F3AC6 3B6FB8AE CF99371F 00F3B053 7CF96D44
        7B10A595 CC60EC48 74F476CE 60175602 3AB93E07 53A049B6
        45708A21 F2322D47 ACF1E2EC AD9731CA 7B7335F4 AB1B03B8


Z is
        03E43CE9 090F3AC6 3B6FB8AE CF99371F 00F3B053 7CF96D44
        7B10A595 CC60EC48 74F476CE 60175602 3AB93E07 53A049B6
        45708A21 F2322D47 ACF1E2EC AD9731CA 7B7335F4 AB1B03B8
        07060501 2021D902 A25C59CA D8D2DFA1 4545C6C6 5A45B26B
        8F3D3812 84F10213 58859BA3 2E0B9666 A72AFF29 7A14203B
        FB630E2F FAA896C2 34A04802 B4862806 07F2B1DD 4013A201


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         180ECF36 89813BC5 397C86FD A3419BF3
        2922F048 88FD9B29 7CB0FADA 7EF5E180 762DFEB8 91B1AAC6
        93D04E7F 7272D5C1 8CF96111 C894D3E3 A03AFC7B 6A88F1CF
        CEEB9DF7 024A872C A35B1FA7 C9E95D34 05572484 3054B600
        20AA2E00 80E9FB2B CEAC66B4 68D7E218 93265CB6 770C8890
        02117294 B818273B B6E8CAF1 119FE4C7 8A00C2C0 EAFD66F3
        5581F0EB A040FD2B C3751560 935B2874 FC8D18D5 5FF71FFC


U2V
----------------
MacData is
                         4B435F32 5F55414C 49434542 4F424259
        077192C3 24FDDF48 74D8B788 244F004F 30FD9A85 9CDB919E
        97CFAE95 16A2703B 56B1EDB8 8D53C17E 3F1A0F4B AF21DA3B
        8ED082BD FE53ACEF F6BB4DE6 93DD4209 DD2D1289 1B594C4C
        05D56CA3 56C46D67 2E8A73CD D02164B7 7A3C54CC 1306B270
        00C70545 3F56BB41 4B191BA3 AE3E2FC1 85AFF2A7 873354DE
        60A21538 039460C3 82456E4C 04FECE44 289F1DFD FE6FB4DE
```

024DB1B7 735FD38B 790E3417 BDFD156B 2F540F89 183B35D1
3A982827 7D9B0C8D D99C3261 07E8F8A1 27EC70BC ACA0C8AB
D59D5A15 0BF8C0CF 81C82DDE FC29B90C E6A65890 9C37AE00
0067E1B3 45827EA0 A4E45CB7 2367C8E5 260A8680 6DFED31C
C7DAEC9A 794AA6D4 C1680494 29CAFD82 70C498DF 411B4888
8244268D 9F1D5F6F 494BD092 8ABDB1EF DD3D6E3D FA2F8305

MacKey is
180ECF36 89813BC5
397C86FD A3419BF3 2922F048 88FD9B29 7CB0FADA 7EF5E180

Mtag is
BE0AD23D 5BE1ED8A 1EEFB7A3 05AAC96E
5FEA7A4D DC105696 64B8FB64 104DD157 F23640AA 57FE575F
81C00C33 53E376A9 F771D7BC 5FBE262E 53FDA6A1 0789A109

V2U

MacData is
4B435F32 5F56424F 42425941 4C494345
024DB1B7 735FD38B 790E3417 BDFD156B 2F540F89 183B35D1
3A982827 7D9B0C8D D99C3261 07E8F8A1 27EC70BC ACA0C8AB
D59D5A15 0BF8C0CF 81C82DDE FC29B90C E6A65890 9C37AE00
0067E1B3 45827EA0 A4E45CB7 2367C8E5 260A8680 6DFED31C
C7DAEC9A 794AA6D4 C1680494 29CAFD82 70C498DF 411B4888
8244268D 9F1D5F6F 494BD092 8ABDB1EF DD3D6E3D FA2F8305
077192C3 24FDDF48 74D8B788 244F004F 30FD9A85 9CDB919E
97CFAE95 16A2703B 56B1EDB8 8D53C17E 3F1A0F4B AF21DA3B
8ED082BD FE53ACEF F6BB4DE6 93DD4209 DD2D1289 1B594C4C
05D56CA3 56C46D67 2E8A73CD D02164B7 7A3C54CC 1306B270
00C70545 3F56BB41 4B191BA3 AE3E2FC1 85AFF2A7 873354DE
60A21538 039460C3 82456E4C 04FECE44 289F1DFD FE6FB4DE

MacKey is
180ECF36 89813BC5
397C86FD A3419BF3 2922F048 88FD9B29 7CB0FADA 7EF5E180

Mtag is
8D790D51 75FF0EB0 BFE3E816 C6F1F87B
8DB58498 85870905 CE36CE97 9DB824D8 E96D621B FF93F1AA
D6627A0E 10B65FB9 90ED0891 944C6A6F 8B9D66F5 2857E6F5

KeyData is
                                                762DFEB8 91B1AAC6
        93D04E7F 7272D5C1 8CF96111 C894D3E3 A03AFC7B 6A88F1CF
        CEEB9DF7 024A872C A35B1FA7 C9E95D34 05572484 3054B600
        20AA2E00 80E9FB2B CEAC66B4 68D7E218 93265CB6 770C8890
        02117294 B818273B B6E8CAF1 119FE4C7 8A00C2C0 EAFD66F3
        5581F0EB A040FD2B C3751560 935B2874 FC8D18D5 5FF71FFC

FullMQV(B-571)
----
dsU is
        009B592D 32F99420 05A38021 D26E7AA6 ED3E78BB DFF2A861
        311B89C9 9DF67762 8EE47F41 AE6A231F 90B13028 98478B30
        FB2F883C 29CD681D 376A9FA6 7AE2FAEB FC7A4B59 440D84F7

QsU_x is
        04B1D9CD E0F54AAC 99E02B4A B0B0705C 2CAF033B C44C1304
        04066DCA DA8E0783 24CBADEE 20B23C91 46F3B0CC 60CD947D
        AD7AA111 C7269CBB FBB6B776 B5F61433 C8F5451B 0E221457

QsU_y is
        0050459A AA86CD0B B4260071 9DBB9505 A6FE6CED 59CFC1A7
        4104845C EC957A88 D15A53C9 2DF39B52 B0060082 BD9B3203
        DBE10B82 0B77BBFA 5694AB23 E33FFC56 5831F5BC 1E479199

dsV is
        01823854 AF10876C 19AEE8EC 6691AD9E 7E294860 5347F7DF
        0EB770FE EB2E71B9 8FAB3273 F7DB3994 AE86986A 7D5533F3
        7556EE07 7B1F9270 A1B990CA 10296BA3 7632CD9F D2F43B6B

QsV_x is
        0431E29F 977CDEA2 90E063C8 3F6B4A0D E33D083C C1844BC4
        60303F63 53FB2B86 888C1BA7 81F89A6E FFA2447C F1E4E772
        E77E8FF6 3243DE77 1692EB0B AE333456 8CF11AE0 9422916F

QsV_y is

01530D05 C336B8C0 121149A2 3416951E D557A58E 4F2A6F64
3CFBA1F1 D508C329 100302D2 BB783676 E0AECE33 EBA2FBFC
8057E158 D9447DC6 D6BF523D 3077CAB6 9590871E C80155B1

deU is
013AC597 40DDBC84 E4803312 4D269467 71CC4872 706EF9F6
34CE0E8A F1A227E8 E14A0898 53A989E5 BE24D464 0D4D6947
884A7936 2618DA2A 14AC7EEB 06DC5BEE C9775477 444EA803

QeU_x is
077192C3 24FDDF48 74D8B788 244F004F 30FD9A85 9CDB919E
97CFAE95 16A2703B 56B1EDB8 8D53C17E 3F1A0F4B AF21DA3B
8ED082BD FE53ACEF F6BB4DE6 93DD4209 DD2D1289 1B594C4C

QeU_y is
05D56CA3 56C46D67 2E8A73CD D02164B7 7A3C54CC 1306B270
00C70545 3F56BB41 4B191BA3 AE3E2FC1 85AFF2A7 873354DE
60A21538 039460C3 82456E4C 04FECE44 289F1DFD FE6FB4DE

deV is
0035076B C0FAE543 F8E32E41 3BD442A5 4EF489B8 9927B021
0360F83F 8703C448 C72F4558 9051B18E B65E1FAE 250BBFEA
6DC924B8 DCD4893F 66DFC547 2479B3AB ADA7E32B C6EF6672

QeV_x is
024DB1B7 735FD38B 790E3417 BDFD156B 2F540F89 183B35D1
3A982827 7D9B0C8D D99C3261 07E8F8A1 27EC70BC ACA0C8AB
D59D5A15 0BF8C0CF 81C82DDE FC29B90C E6A65890 9C37AE00

QeV_y is
0067E1B3 45827EA0 A4E45CB7 2367C8E5 260A8680 6DFED31C
C7DAEC9A 794AA6D4 C1680494 29CAFD82 70C498DF 411B4888
8244268D 9F1D5F6F 494BD092 8ABDB1EF DD3D6E3D FA2F8305

---

no Key Confirmation
Z is

```
        0390AEEA 424BEE7C 28E2CA85 63D6D043 DE8A1C0B 431D0A58
        EB2CCA30 7D86FA73 3007BAE5 47524F5B C9042A0E 5474E725
        00C5CAEE 94A53996 6F40FDC8 615899E3 D3569773 594982D2


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                5D97E442 E10D7041
        6C9A0035 2248A76F 385142F7 E63B00EB 360DAF75 CCC1F4F7
        643AAD15 424A90F0 DDFA8973 1D3F9C64 DF43392D A449E80A
        E80FF25E B36EDDA9 D0DAD47D E22B52DF E083E7D8 65C04DDF
        8A4C19EA 9D023483 E836C901 C8E48D5C D01A4CB5 D8A848FE
        38226702 B7EA98D7 054748FE 1A5C63E2 93A0539C 4749C11A


KeyData is
                                                5D97E442 E10D7041
        6C9A0035 2248A76F 385142F7 E63B00EB 360DAF75 CCC1F4F7
        643AAD15 424A90F0 DDFA8973 1D3F9C64 DF43392D A449E80A
        E80FF25E B36EDDA9 D0DAD47D E22B52DF E083E7D8 65C04DDF
        8A4C19EA 9D023483 E836C901 C8E48D5C D01A4CB5 D8A848FE
        38226702 B7EA98D7 054748FE 1A5C63E2 93A0539C 4749C11A




-------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Z is
        0390AEEA 424BEE7C 28E2CA85 63D6D043 DE8A1C0B 431D0A58
        EB2CCA30 7D86FA73 3007BAE5 47524F5B C9042A0E 5474E725
        00C5CAEE 94A53996 6F40FDC8 615899E3 D3569773 594982D2


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                            5D97E442 E10D7041 6C9A0035 2248A76F
        385142F7 E63B00EB 360DAF75 CCC1F4F7 643AAD15 424A90F0
        DDFA8973 1D3F9C64 DF43392D A449E80A E80FF25E B36EDDA9
        D0DAD47D E22B52DF E083E7D8 65C04DDF 8A4C19EA 9D023483
```

```
        E836C901 C8E48D5C D01A4CB5 D8A848FE 38226702 B7EA98D7
        054748FE 1A5C63E2 93A0539C 4749C11A 9CC60AD5 5B7FB5F0
        8152718B F24A4261 7E98F8BE 745936A9 EDE9A099 872271D2


MacData is
                         4B435F31 5F55414C 49434542 4F424259
        077192C3 24FDDF48 74D8B788 244F004F 30FD9A85 9CDB919E
        97CFAE95 16A2703B 56B1EDB8 8D53C17E 3F1A0F4B AF21DA3B
        8ED082BD FE53ACEF F6BB4DE6 93DD4209 DD2D1289 1B594C4C
        05D56CA3 56C46D67 2E8A73CD D02164B7 7A3C54CC 1306B270
        00C70545 3F56BB41 4B191BA3 AE3E2FC1 85AFF2A7 873354DE
        60A21538 039460C3 82456E4C 04FECE44 289F1DFD FE6FB4DE
        024DB1B7 735FD38B 790E3417 BDFD156B 2F540F89 183B35D1
        3A982827 7D9B0C8D D99C3261 07E8F8A1 27EC70BC ACA0C8AB
        D59D5A15 0BF8C0CF 81C82DDE FC29B90C E6A65890 9C37AE00
        0067E1B3 45827EA0 A4E45CB7 2367C8E5 260A8680 6DFED31C
        C7DAEC9A 794AA6D4 C1680494 29CAFD82 70C498DF 411B4888
        8244268D 9F1D5F6F 494BD092 8ABDB1EF DD3D6E3D FA2F8305


MacKey is
                                                 5D97E442 E10D7041
        6C9A0035 2248A76F 385142F7 E63B00EB 360DAF75 CCC1F4F7


Mtag is
                         93D72D3A F5D8822C AA18FD3F DABE5CF3
        69C1048A CF402E09 D9533E26 E6962809 A3355114 2B56D89C
        C6B1D7EE F3438C92 18D2D3D5 B72046B1 D27E42CB 8B41AFC1


KeyData is
                                                 643AAD15 424A90F0
        DDFA8973 1D3F9C64 DF43392D A449E80A E80FF25E B36EDDA9
        D0DAD47D E22B52DF E083E7D8 65C04DDF 8A4C19EA 9D023483
        E836C901 C8E48D5C D01A4CB5 D8A848FE 38226702 B7EA98D7
        054748FE 1A5C63E2 93A0539C 4749C11A 9CC60AD5 5B7FB5F0
        8152718B F24A4261 7E98F8BE 745936A9 EDE9A099 872271D2




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
```

```
        0390AEEA 424BEE7C 28E2CA85 63D6D043 DE8A1C0B 431D0A58
        EB2CCA30 7D86FA73 3007BAE5 47524F5B C9042A0E 5474E725
        00C5CAEE 94A53996 6F40FDC8 615899E3 D3569773 594982D2


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         5D97E442 E10D7041 6C9A0035 2248A76F
        385142F7 E63B00EB 360DAF75 CCC1F4F7 643AAD15 424A90F0
        DDFA8973 1D3F9C64 DF43392D A449E80A E80FF25E B36EDDA9
        D0DAD47D E22B52DF E083E7D8 65C04DDF 8A4C19EA 9D023483
        E836C901 C8E48D5C D01A4CB5 D8A848FE 38226702 B7EA98D7
        054748FE 1A5C63E2 93A0539C 4749C11A 9CC60AD5 5B7FB5F0
        8152718B F24A4261 7E98F8BE 745936A9 EDE9A099 872271D2


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        024DB1B7 735FD38B 790E3417 BDFD156B 2F540F89 183B35D1
        3A982827 7D9B0C8D D99C3261 07E8F8A1 27EC70BC ACA0C8AB
        D59D5A15 0BF8C0CF 81C82DDE FC29B90C E6A65890 9C37AE00
        0067E1B3 45827EA0 A4E45CB7 2367C8E5 260A8680 6DFED31C
        C7DAEC9A 794AA6D4 C1680494 29CAFD82 70C498DF 411B4888
        8244268D 9F1D5F6F 494BD092 8ABDB1EF DD3D6E3D FA2F8305
        077192C3 24FDDF48 74D8B788 244F004F 30FD9A85 9CDB919E
        97CFAE95 16A2703B 56B1EDB8 8D53C17E 3F1A0F4B AF21DA3B
        8ED082BD FE53ACEF F6BB4DE6 93DD4209 DD2D1289 1B594C4C
        05D56CA3 56C46D67 2E8A73CD D02164B7 7A3C54CC 1306B270
        00C70545 3F56BB41 4B191BA3 AE3E2FC1 85AFF2A7 873354DE
        60A21538 039460C3 82456E4C 04FECE44 289F1DFD FE6FB4DE


MacKey is
                                                 5D97E442 E10D7041
        6C9A0035 2248A76F 385142F7 E63B00EB 360DAF75 CCC1F4F7


Mtag is
                         D0957256 4C3B47DF 3EF570D8 438B4F84
        32924C89 FDFC2EDF 40960581 5BE7CC1B 51C7CFC0 AA0E546B
        B5933E72 F9976EFD E86F88EF 626FF5B3 FA148256 B6C80FAE
```

KeyData is
                                                643AAD15 424A90F0
        DDFA8973 1D3F9C64 DF43392D A449E80A E80FF25E B36EDDA9
        D0DAD47D E22B52DF E083E7D8 65C04DDF 8A4C19EA 9D023483
        E836C901 C8E48D5C D01A4CB5 D8A848FE 38226702 B7EA98D7
        054748FE 1A5C63E2 93A0539C 4749C11A 9CC60AD5 5B7FB5F0
        8152718B F24A4261 7E98F8BE 745936A9 EDE9A099 872271D2

Scheme Initiator, Key Confirmation Bilateral
Z is
        0390AEEA 424BEE7C 28E2CA85 63D6D043 DE8A1C0B 431D0A58
        EB2CCA30 7D86FA73 3007BAE5 47524F5B C9042A0E 5474E725
        00C5CAEE 94A53996 6F40FDC8 615899E3 D3569773 594982D2

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                         5D97E442 E10D7041 6C9A0035 2248A76F
        385142F7 E63B00EB 360DAF75 CCC1F4F7 643AAD15 424A90F0
        DDFA8973 1D3F9C64 DF43392D A449E80A E80FF25E B36EDDA9
        D0DAD47D E22B52DF E083E7D8 65C04DDF 8A4C19EA 9D023483
        E836C901 C8E48D5C D01A4CB5 D8A848FE 38226702 B7EA98D7
        054748FE 1A5C63E2 93A0539C 4749C11A 9CC60AD5 5B7FB5F0
        8152718B F24A4261 7E98F8BE 745936A9 EDE9A099 872271D2

U2V

MacData is
                         4B435F32 5F55414C 49434542 4F424259
        077192C3 24FDDF48 74D8B788 244F004F 30FD9A85 9CDB919E
        97CFAE95 16A2703B 56B1EDB8 8D53C17E 3F1A0F4B AF21DA3B
        8ED082BD FE53ACEF F6BB4DE6 93DD4209 DD2D1289 1B594C4C
        05D56CA3 56C46D67 2E8A73CD D02164B7 7A3C54CC 1306B270
        00C70545 3F56BB41 4B191BA3 AE3E2FC1 85AFF2A7 873354DE
        60A21538 039460C3 82456E4C 04FECE44 289F1DFD FE6FB4DE
        024DB1B7 735FD38B 790E3417 BDFD156B 2F540F89 183B35D1
        3A982827 7D9B0C8D D99C3261 07E8F8A1 27EC70BC ACA0C8AB

```
        D59D5A15 0BF8C0CF 81C82DDE FC29B90C E6A65890 9C37AE00
        0067E1B3 45827EA0 A4E45CB7 2367C8E5 260A8680 6DFED31C
        C7DAEC9A 794AA6D4 C1680494 29CAFD82 70C498DF 411B4888
        8244268D 9F1D5F6F 494BD092 8ABDB1EF DD3D6E3D FA2F8305


MacKey is
                                                5D97E442 E10D7041
        6C9A0035 2248A76F 385142F7 E63B00EB 360DAF75 CCC1F4F7


Mtag is
                         94739508 4A244D1F A90E1B35 D68FCF61
        4C07ED72 737A8B66 4CEBEA96 67A9B016 B8105A58 E93959C2
        FF24D3AB CA1463DB 3F610975 E7A0C223 3385DF7B 4D3D778C


V2U
----------------
MacData is
                         4B435F32 5F56424F 42425941 4C494345
        024DB1B7 735FD38B 790E3417 BDFD156B 2F540F89 183B35D1
        3A982827 7D9B0C8D D99C3261 07E8F8A1 27EC70BC ACA0C8AB
        D59D5A15 0BF8C0CF 81C82DDE FC29B90C E6A65890 9C37AE00
        0067E1B3 45827EA0 A4E45CB7 2367C8E5 260A8680 6DFED31C
        C7DAEC9A 794AA6D4 C1680494 29CAFD82 70C498DF 411B4888
        8244268D 9F1D5F6F 494BD092 8ABDB1EF DD3D6E3D FA2F8305
        077192C3 24FDDF48 74D8B788 244F004F 30FD9A85 9CDB919E
        97CFAE95 16A2703B 56B1EDB8 8D53C17E 3F1A0F4B AF21DA3B
        8ED082BD FE53ACEF F6BB4DE6 93DD4209 DD2D1289 1B594C4C
        05D56CA3 56C46D67 2E8A73CD D02164B7 7A3C54CC 1306B270
        00C70545 3F56BB41 4B191BA3 AE3E2FC1 85AFF2A7 873354DE
        60A21538 039460C3 82456E4C 04FECE44 289F1DFD FE6FB4DE


MacKey is
                                                5D97E442 E10D7041
        6C9A0035 2248A76F 385142F7 E63B00EB 360DAF75 CCC1F4F7


Mtag is
                         5B0A3962 9236DA29 8384A289 B8EC44F1
        F68870CE EDD225B5 1A0550FB A6C6D9D0 C419FD29 B4D8FE1A
        53A6B80E E2610EBE FF436F20 A6D20282 2D74A447 87085BBD
```

```
KeyData is
                                                643AAD15 424A90F0
        DDFA8973 1D3F9C64 DF43392D A449E80A E80FF25E B36EDDA9
        D0DAD47D E22B52DF E083E7D8 65C04DDF 8A4C19EA 9D023483
        E836C901 C8E48D5C D01A4CB5 D8A848FE 38226702 B7EA98D7
        054748FE 1A5C63E2 93A0539C 4749C11A 9CC60AD5 5B7FB5F0
        8152718B F24A4261 7E98F8BE 745936A9 EDE9A099 872271D2



EphemeralUnifiedCDH(B-571)
------------------------------------------------------------
deU is
        013AC597 40DDBC84 E4803312 4D269467 71CC4872 706EF9F6
        34CE0E8A F1A227E8 E14A0898 53A989E5 BE24D464 0D4D6947
        884A7936 2618DA2A 14AC7EEB 06DC5BEE C9775477 444EA803


QeU_x is
        077192C3 24FDDF48 74D8B788 244F004F 30FD9A85 9CDB919E
        97CFAE95 16A2703B 56B1EDB8 8D53C17E 3F1A0F4B AF21DA3B
        8ED082BD FE53ACEF F6BB4DE6 93DD4209 DD2D1289 1B594C4C


QeU_y is
        05D56CA3 56C46D67 2E8A73CD D02164B7 7A3C54CC 1306B270
        00C70545 3F56BB41 4B191BA3 AE3E2FC1 85AFF2A7 873354DE
        60A21538 039460C3 82456E4C 04FECE44 289F1DFD FE6FB4DE


deV is
        0035076B C0FAE543 F8E32E41 3BD442A5 4EF489B8 9927B021
        0360F83F 8703C448 C72F4558 9051B18E B65E1FAE 250BBFEA
        6DC924B8 DCD4893F 66DFC547 2479B3AB ADA7E32B C6EF6672


QeV_x is
        024DB1B7 735FD38B 790E3417 BDFD156B 2F540F89 183B35D1
        3A982827 7D9B0C8D D99C3261 07E8F8A1 27EC70BC ACA0C8AB
        D59D5A15 0BF8C0CF 81C82DDE FC29B90C E6A65890 9C37AE00


QeV_y is
        0067E1B3 45827EA0 A4E45CB7 2367C8E5 260A8680 6DFED31C
        C7DAEC9A 794AA6D4 C1680494 29CAFD82 70C498DF 411B4888
```

8244268D 9F1D5F6F 494BD092 8ABDB1EF DD3D6E3D FA2F8305

---

no Key Confirmation
Z is
03E43CE9 090F3AC6 3B6FB8AE CF99371F 00F3B053 7CF96D44
7B10A595 CC60EC48 74F476CE 60175602 3AB93E07 53A049B6
45708A21 F2322D47 ACF1E2EC AD9731CA 7B7335F4 AB1B03B8

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
3592C41C 5D198C5D
C52294F4 CDC44992 DE8E761E 57F6CFB9 E84A2F21 6776E3B2
4B159840 E127752F 5822317F 6B070895 F4B8679D 2FE589D0
C5752086 7CDEFEE7 788E9C6A C9342CE6 B5ABC5CF A4F07912
424452A2 7B09F329 911E23A3 F80C9D32 EE0B03C4 EDE41A44
703F9141 0463F6B4 7B73665A 5FD9A972 3CB166DA D0AC804C

KeyData is
3592C41C 5D198C5D
C52294F4 CDC44992 DE8E761E 57F6CFB9 E84A2F21 6776E3B2
4B159840 E127752F 5822317F 6B070895 F4B8679D 2FE589D0
C5752086 7CDEFEE7 788E9C6A C9342CE6 B5ABC5CF A4F07912
424452A2 7B09F329 911E23A3 F80C9D32 EE0B03C4 EDE41A44
703F9141 0463F6B4 7B73665A 5FD9A972 3CB166DA D0AC804C

OnePassUnifiedCDH(B-571)
---

dsU is
009B592D 32F99420 05A38021 D26E7AA6 ED3E78BB DFF2A861
311B89C9 9DF67762 8EE47F41 AE6A231F 90B13028 98478B30
FB2F883C 29CD681D 376A9FA6 7AE2FAEB FC7A4B59 440D84F7

QsU_x is

04B1D9CD E0F54AAC 99E02B4A B0B0705C 2CAF033B C44C1304
04066DCA DA8E0783 24CBADEE 20B23C91 46F3B0CC 60CD947D
AD7AA111 C7269CBB FBB6B776 B5F61433 C8F5451B 0E221457

QsU_y is
0050459A AA86CD0B B4260071 9DBB9505 A6FE6CED 59CFC1A7
4104845C EC957A88 D15A53C9 2DF39B52 B0060082 BD9B3203
DBE10B82 0B77BBFA 5694AB23 E33FFC56 5831F5BC 1E479199

dsV is
01823854 AF10876C 19AEE8EC 6691AD9E 7E294860 5347F7DF
0EB770FE EB2E71B9 8FAB3273 F7DB3994 AE86986A 7D5533F3
7556EE07 7B1F9270 A1B990CA 10296BA3 7632CD9F D2F43B6B

QsV_x is
0431E29F 977CDEA2 90E063C8 3F6B4A0D E33D083C C1844BC4
60303F63 53FB2B86 888C1BA7 81F89A6E FFA2447C F1E4E772
E77E8FF6 3243DE77 1692EB0B AE333456 8CF11AE0 9422916F

QsV_y is
01530D05 C336B8C0 121149A2 3416951E D557A58E 4F2A6F64
3CFBA1F1 D508C329 100302D2 BB783676 E0AECE33 EBA2FBFC
8057E158 D9447DC6 D6BF523D 3077CAB6 9590871E C80155B1

deU is
013AC597 40DDBC84 E4803312 4D269467 71CC4872 706EF9F6
34CE0E8A F1A227E8 E14A0898 53A989E5 BE24D464 0D4D6947
884A7936 2618DA2A 14AC7EEB 06DC5BEE C9775477 444EA803

QeU_x is
077192C3 24FDDF48 74D8B788 244F004F 30FD9A85 9CDB919E
97CFAE95 16A2703B 56B1EDB8 8D53C17E 3F1A0F4B AF21DA3B
8ED082BD FE53ACEF F6BB4DE6 93DD4209 DD2D1289 1B594C4C

QeU_y is
05D56CA3 56C46D67 2E8A73CD D02164B7 7A3C54CC 1306B270
00C70545 3F56BB41 4B191BA3 AE3E2FC1 85AFF2A7 873354DE
60A21538 039460C3 82456E4C 04FECE44 289F1DFD FE6FB4DE

```
-----------------------------------------------------------
no Key Confirmation
Zs is
        07060501 2021D902 A25C59CA D8D2DFA1 4545C6C6 5A45B26B
        8F3D3812 84F10213 58859BA3 2E0B9666 A72AFF29 7A14203B
        FB630E2F FAA896C2 34A04802 B4862806 07F2B1DD 4013A201


Ze is
        07C93A62 8305A453 88803054 2685F73A 273F5245 B9591F45
        1C3BC32B 35135F14 C00E22A4 C10017A0 D67EC191 5267516E
        E70DCFCB 7DD9748B E73B06AA BD5F6662 4D6B1A8F 84CA2572


Z is
        07C93A62 8305A453 88803054 2685F73A 273F5245 B9591F45
        1C3BC32B 35135F14 C00E22A4 C10017A0 D67EC191 5267516E
        E70DCFCB 7DD9748B E73B06AA BD5F6662 4D6B1A8F 84CA2572
        07060501 2021D902 A25C59CA D8D2DFA1 4545C6C6 5A45B26B
        8F3D3812 84F10213 58859BA3 2E0B9666 A72AFF29 7A14203B
        FB630E2F FAA896C2 34A04802 B4862806 07F2B1DD 4013A201


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                            25409874 779086CF
        CC1563B2 A3A2FF08 2E43810B 5A9E2E94 18081387 B6F56ACF
        0241B84B F869CDB9 B7B2D6A3 CAD3334B 94A91F04 3E487401
        510B5F4F 4910E749 0126673C DF69BC32 E1EE20AA 6A3A6FAC
        FE97F003 CB415A06 C326AE86 A45FE3F8 9547A20A E8F7E3F2
        D9CEB523 C02B4EE6 4B71FEEB 135B812E 67BA89BD B99A6CE3


KeyData is
                                            25409874 779086CF
        CC1563B2 A3A2FF08 2E43810B 5A9E2E94 18081387 B6F56ACF
        0241B84B F869CDB9 B7B2D6A3 CAD3334B 94A91F04 3E487401
        510B5F4F 4910E749 0126673C DF69BC32 E1EE20AA 6A3A6FAC
        FE97F003 CB415A06 C326AE86 A45FE3F8 9547A20A E8F7E3F2
        D9CEB523 C02B4EE6 4B71FEEB 135B812E 67BA89BD B99A6CE3
```

```
------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB80 87548FEE 838A8607 7AFC2DC3
        D5FBFA15 9E92BCE2 5CDE8DE2 624D9002 0AF07F1F 9730194E


Zs is
        07060501 2021D902 A25C59CA D8D2DFA1 4545C6C6 5A45B26B
        8F3D3812 84F10213 58859BA3 2E0B9666 A72AFF29 7A14203B
        FB630E2F FAA896C2 34A04802 B4862806 07F2B1DD 4013A201


Ze is
        07C93A62 8305A453 88803054 2685F73A 273F5245 B9591F45
        1C3BC32B 35135F14 C00E22A4 C10017A0 D67EC191 5267516E
        E70DCFCB 7DD9748B E73B06AA BD5F6662 4D6B1A8F 84CA2572


Z is
        07C93A62 8305A453 88803054 2685F73A 273F5245 B9591F45
        1C3BC32B 35135F14 C00E22A4 C10017A0 D67EC191 5267516E
        E70DCFCB 7DD9748B E73B06AA BD5F6662 4D6B1A8F 84CA2572
        07060501 2021D902 A25C59CA D8D2DFA1 4545C6C6 5A45B26B
        8F3D3812 84F10213 58859BA3 2E0B9666 A72AFF29 7A14203B
        FB630E2F FAA896C2 34A04802 B4862806 07F2B1DD 4013A201


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         25409874 779086CF CC1563B2 A3A2FF08
        2E43810B 5A9E2E94 18081387 B6F56ACF 0241B84B F869CDB9
        B7B2D6A3 CAD3334B 94A91F04 3E487401 510B5F4F 4910E749
        0126673C DF69BC32 E1EE20AA 6A3A6FAC FE97F003 CB415A06
        C326AE86 A45FE3F8 9547A20A E8F7E3F2 D9CEB523 C02B4EE6
        4B71FEEB 135B812E 67BA89BD B99A6CE3 855895F2 DD9699D4
        E5A225F1 092A5540 64ED3706 EB9C8EFA DD21403F C30B40E9
```

```
MacData is
                          4B435F31 5F55414C 49434542 4F424259
        077192C3 24FDDF48 74D8B788 244F004F 30FD9A85 9CDB919E
        97CFAE95 16A2703B 56B1EDB8 8D53C17E 3F1A0F4B AF21DA3B
        8ED082BD FE53ACEF F6BB4DE6 93DD4209 DD2D1289 1B594C4C
        05D56CA3 56C46D67 2E8A73CD D02164B7 7A3C54CC 1306B270
        00C70545 3F56BB41 4B191BA3 AE3E2FC1 85AFF2A7 873354DE
        60A21538 039460C3 82456E4C 04FECE44 289F1DFD FE6FB4DE
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB80 87548FEE 838A8607 7AFC2DC3
        D5FBFA15 9E92BCE2 5CDE8DE2 624D9002 0AF07F1F 9730194E


MacKey is
                                                  25409874 779086CF
        CC1563B2 A3A2FF08 2E43810B 5A9E2E94 18081387 B6F56ACF


Mtag is
                          A687DF32 609601CD B8AE300D 5A037235
        426BF71B B93EA380 2C1DAC3C 9C78DFFE 265E9FDE B9B44C03
        D0B2D825 344FB858 0443CA1C DA350797 4D57A99D 30B455FA


KeyData is
                                                  0241B84B F869CDB9
        B7B2D6A3 CAD3334B 94A91F04 3E487401 510B5F4F 4910E749
        0126673C DF69BC32 E1EE20AA 6A3A6FAC FE97F003 CB415A06
        C326AE86 A45FE3F8 9547A20A E8F7E3F2 D9CEB523 C02B4EE6
        4B71FEEB 135B812E 67BA89BD B99A6CE3 855895F2 DD9699D4
        E5A225F1 092A5540 64ED3706 EB9C8EFA DD21403F C30B40E9




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB80 87548FEE 838A8607 7AFC2DC3
        D5FBFA15 9E92BCE2 5CDE8DE2 624D9002 0AF07F1F 9730194E


Zs is
        07060501 2021D902 A25C59CA D8D2DFA1 4545C6C6 5A45B26B
```

8F3D3812 84F10213 58859BA3 2E0B9666 A72AFF29 7A14203B
FB630E2F FAA896C2 34A04802 B4862806 07F2B1DD 4013A201

Ze is
07C93A62 8305A453 88803054 2685F73A 273F5245 B9591F45
1C3BC32B 35135F14 C00E22A4 C10017A0 D67EC191 5267516E
E70DCFCB 7DD9748B E73B06AA BD5F6662 4D6B1A8F 84CA2572

Z is
07C93A62 8305A453 88803054 2685F73A 273F5245 B9591F45
1C3BC32B 35135F14 C00E22A4 C10017A0 D67EC191 5267516E
E70DCFCB 7DD9748B E73B06AA BD5F6662 4D6B1A8F 84CA2572
07060501 2021D902 A25C59CA D8D2DFA1 4545C6C6 5A45B26B
8F3D3812 84F10213 58859BA3 2E0B9666 A72AFF29 7A14203B
FB630E2F FAA896C2 34A04802 B4862806 07F2B1DD 4013A201

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
25409874 779086CF CC1563B2 A3A2FF08
2E43810B 5A9E2E94 18081387 B6F56ACF 0241B84B F869CDB9
B7B2D6A3 CAD3334B 94A91F04 3E487401 510B5F4F 4910E749
0126673C DF69BC32 E1EE20AA 6A3A6FAC FE97F003 CB415A06
C326AE86 A45FE3F8 9547A20A E8F7E3F2 D9CEB523 C02B4EE6
4B71FEEB 135B812E 67BA89BD B99A6CE3 855895F2 DD9699D4
E5A225F1 092A5540 64ED3706 EB9C8EFA DD21403F C30B40E9

MacData is
4B435F31 5F56424F 42425941 4C494345
077192C3 24FDDF48 74D8B788 244F004F 30FD9A85 9CDB919E
97CFAE95 16A2703B 56B1EDB8 8D53C17E 3F1A0F4B AF21DA3B
8ED082BD FE53ACEF F6BB4DE6 93DD4209 DD2D1289 1B594C4C
05D56CA3 56C46D67 2E8A73CD D02164B7 7A3C54CC 1306B270
00C70545 3F56BB41 4B191BA3 AE3E2FC1 85AFF2A7 873354DE
60A21538 039460C3 82456E4C 04FECE44 289F1DFD FE6FB4DE

MacKey is
25409874 779086CF
CC1563B2 A3A2FF08 2E43810B 5A9E2E94 18081387 B6F56ACF

```
Mtag is
                        F207E8A8 985DF5CA 49FA841D 00D4DAEF
        F300936F 3AA78570 FA2E947B 4DDA5724 1B88C1B0 A45E7E01
        1405EE1F 0FB29B6B 303423F4 F319BCA1 0CF854AB 286355A1


KeyData is
                                                 0241B84B F869CDB9
        B7B2D6A3 CAD3334B 94A91F04 3E487401 510B5F4F 4910E749
        0126673C DF69BC32 E1EE20AA 6A3A6FAC FE97F003 CB415A06
        C326AE86 A45FE3F8 9547A20A E8F7E3F2 D9CEB523 C02B4EE6
        4B71FEEB 135B812E 67BA89BD B99A6CE3 855895F2 DD9699D4
        E5A225F1 092A5540 64ED3706 EB9C8EFA DD21403F C30B40E9




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB80 87548FEE 838A8607 7AFC2DC3
        D5FBFA15 9E92BCE2 5CDE8DE2 624D9002 0AF07F1F 9730194E


Zs is
        07060501 2021D902 A25C59CA D8D2DFA1 4545C6C6 5A45B26B
        8F3D3812 84F10213 58859BA3 2E0B9666 A72AFF29 7A14203B
        FB630E2F FAA896C2 34A04802 B4862806 07F2B1DD 4013A201


Ze is
        07C93A62 8305A453 88803054 2685F73A 273F5245 B9591F45
        1C3BC32B 35135F14 C00E22A4 C10017A0 D67EC191 5267516E
        E70DCFCB 7DD9748B E73B06AA BD5F6662 4D6B1A8F 84CA2572


Z is
        07C93A62 8305A453 88803054 2685F73A 273F5245 B9591F45
        1C3BC32B 35135F14 C00E22A4 C10017A0 D67EC191 5267516E
        E70DCFCB 7DD9748B E73B06AA BD5F6662 4D6B1A8F 84CA2572
        07060501 2021D902 A25C59CA D8D2DFA1 4545C6C6 5A45B26B
        8F3D3812 84F10213 58859BA3 2E0B9666 A72AFF29 7A14203B
        FB630E2F FAA896C2 34A04802 B4862806 07F2B1DD 4013A201
```

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         25409874 779086CF CC1563B2 A3A2FF08
        2E43810B 5A9E2E94 18081387 B6F56ACF 0241B84B F869CDB9
        B7B2D6A3 CAD3334B 94A91F04 3E487401 510B5F4F 4910E749
        0126673C DF69BC32 E1EE20AA 6A3A6FAC FE97F003 CB415A06
        C326AE86 A45FE3F8 9547A20A E8F7E3F2 D9CEB523 C02B4EE6
        4B71FEEB 135B812E 67BA89BD B99A6CE3 855895F2 DD9699D4
        E5A225F1 092A5540 64ED3706 EB9C8EFA DD21403F C30B40E9


U2V
----------------
MacData is
                         4B435F32 5F55414C 49434542 4F424259
        077192C3 24FDDF48 74D8B788 244F004F 30FD9A85 9CDB919E
        97CFAE95 16A2703B 56B1EDB8 8D53C17E 3F1A0F4B AF21DA3B
        8ED082BD FE53ACEF F6BB4DE6 93DD4209 DD2D1289 1B594C4C
        05D56CA3 56C46D67 2E8A73CD D02164B7 7A3C54CC 1306B270
        00C70545 3F56BB41 4B191BA3 AE3E2FC1 85AFF2A7 873354DE
        60A21538 039460C3 82456E4C 04FECE44 289F1DFD FE6FB4DE
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB80 87548FEE 838A8607 7AFC2DC3
        D5FBFA15 9E92BCE2 5CDE8DE2 624D9002 0AF07F1F 9730194E


MacKey is
                                                 25409874 779086CF
        CC1563B2 A3A2FF08 2E43810B 5A9E2E94 18081387 B6F56ACF


Mtag is
                         928DEB87 2AEE0814 3BD4EF67 9B910528
        EF193F41 68CD14E8 8B5DAF6B 27F7FADF 257F44F7 4AE75CD5
        3146825D 71FFBC66 4D642013 91424277 E24E45E6 9579FA11


V2U
----------------
MacData is
                         4B435F32 5F56424F 42425941 4C494345
```

```
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB80 87548FEE 838A8607 7AFC2DC3
        D5FBFA15 9E92BCE2 5CDE8DE2 624D9002 0AF07F1F 9730194E
        077192C3 24FDDF48 74D8B788 244F004F 30FD9A85 9CDB919E
        97CFAE95 16A2703B 56B1EDB8 8D53C17E 3F1A0F4B AF21DA3B
        8ED082BD FE53ACEF F6BB4DE6 93DD4209 DD2D1289 1B594C4C
        05D56CA3 56C46D67 2E8A73CD D02164B7 7A3C54CC 1306B270
        00C70545 3F56BB41 4B191BA3 AE3E2FC1 85AFF2A7 873354DE
        60A21538 039460C3 82456E4C 04FECE44 289F1DFD FE6FB4DE


MacKey is
                                            25409874 779086CF
        CC1563B2 A3A2FF08 2E43810B 5A9E2E94 18081387 B6F56ACF


Mtag is
                         6B3D0341 AE6D3DAE E400A02E 91B7E14E
        0B500B30 CEAE5C77 0B7EDEB4 7775F9EA 29708FE5 424B73C4
        7F8E14D7 0F9EBBE2 2BCAF487 18A7D8F7 A664B413 3EA105C0


KeyData is
                                            0241B84B F869CDB9
        B7B2D6A3 CAD3334B 94A91F04 3E487401 510B5F4F 4910E749
        0126673C DF69BC32 E1EE20AA 6A3A6FAC FE97F003 CB415A06
        C326AE86 A45FE3F8 9547A20A E8F7E3F2 D9CEB523 C02B4EE6
        4B71FEEB 135B812E 67BA89BD B99A6CE3 855895F2 DD9699D4
        E5A225F1 092A5540 64ED3706 EB9C8EFA DD21403F C30B40E9




OnePassMQV(B-571)
------------------------------------------------------------
dsU is
        009B592D 32F99420 05A38021 D26E7AA6 ED3E78BB DFF2A861
        311B89C9 9DF67762 8EE47F41 AE6A231F 90B13028 98478B30
        FB2F883C 29CD681D 376A9FA6 7AE2FAEB FC7A4B59 440D84F7


QsU_x is
        04B1D9CD E0F54AAC 99E02B4A B0B0705C 2CAF033B C44C1304
        04066DCA DA8E0783 24CBADEE 20B23C91 46F3B0CC 60CD947D
        AD7AA111 C7269CBB FBB6B776 B5F61433 C8F5451B 0E221457
```

```
QsU_y is
        0050459A AA86CD0B B4260071 9DBB9505 A6FE6CED 59CFC1A7
        4104845C EC957A88 D15A53C9 2DF39B52 B0060082 BD9B3203
        DBE10B82 0B77BBFA 5694AB23 E33FFC56 5831F5BC 1E479199


dsV is
        01823854 AF10876C 19AEE8EC 6691AD9E 7E294860 5347F7DF
        0EB770FE EB2E71B9 8FAB3273 F7DB3994 AE86986A 7D5533F3
        7556EE07 7B1F9270 A1B990CA 10296BA3 7632CD9F D2F43B6B


QsV_x is
        0431E29F 977CDEA2 90E063C8 3F6B4A0D E33D083C C1844BC4
        60303F63 53FB2B86 888C1BA7 81F89A6E FFA2447C F1E4E772
        E77E8FF6 3243DE77 1692EB0B AE333456 8CF11AE0 9422916F


QsV_y is
        01530D05 C336B8C0 121149A2 3416951E D557A58E 4F2A6F64
        3CFBA1F1 D508C329 100302D2 BB783676 E0AECE33 EBA2FBFC
        8057E158 D9447DC6 D6BF523D 3077CAB6 9590871E C80155B1


deU is
        013AC597 40DDBC84 E4803312 4D269467 71CC4872 706EF9F6
        34CE0E8A F1A227E8 E14A0898 53A989E5 BE24D464 0D4D6947
        884A7936 2618DA2A 14AC7EEB 06DC5BEE C9775477 444EA803


QeU_x is
        077192C3 24FDDF48 74D8B788 244F004F 30FD9A85 9CDB919E
        97CFAE95 16A2703B 56B1EDB8 8D53C17E 3F1A0F4B AF21DA3B
        8ED082BD FE53ACEF F6BB4DE6 93DD4209 DD2D1289 1B594C4C


QeU_y is
        05D56CA3 56C46D67 2E8A73CD D02164B7 7A3C54CC 1306B270
        00C70545 3F56BB41 4B191BA3 AE3E2FC1 85AFF2A7 873354DE
        60A21538 039460C3 82456E4C 04FECE44 289F1DFD FE6FB4DE



------------------------------------------------------------
```

```
no Key Confirmation
Z is
        0050180B DA7D8F75 08DC8D59 6D74136E 961CF6E4 FF2AC680
        468A9886 E4F65408 3CD006A1 3BE0FD6E 88BAB1D3 C6DF2375
        E1C08BBD 0A7D7F1F 063B7C82 EA8DCC44 170B1411 CA9ED66F


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                            CDFB1507 E397D3DB
        9217ABA3 45EF658D 265DBD98 28F2A91E 6A30EF59 5B099319
        E1884D73 E73417BD F72451F8 AC4618D2 2232F3C7 F9EC13AB
        69AF1F4C 385827BF 498B2248 63A63612 E1860590 3ADB7F12
        AE4B96B2 A7F61FDA D963A733 D9B1CF4D C8A4EA1E B2827485
        B0EE36F6 BF54D63B 299190DA 6C2860F5 39B3E0F9 75C801D3


KeyData is
                                            CDFB1507 E397D3DB
        9217ABA3 45EF658D 265DBD98 28F2A91E 6A30EF59 5B099319
        E1884D73 E73417BD F72451F8 AC4618D2 2232F3C7 F9EC13AB
        69AF1F4C 385827BF 498B2248 63A63612 E1860590 3ADB7F12
        AE4B96B2 A7F61FDA D963A733 D9B1CF4D C8A4EA1E B2827485
        B0EE36F6 BF54D63B 299190DA 6C2860F5 39B3E0F9 75C801D3




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB80 87548FEE 838A8607 7AFC2DC3
        D5FBFA15 9E92BCE2 5CDE8DE2 624D9002 0AF07F1F 9730194E


Z is
        0050180B DA7D8F75 08DC8D59 6D74136E 961CF6E4 FF2AC680
        468A9886 E4F65408 3CD006A1 3BE0FD6E 88BAB1D3 C6DF2375
        E1C08BBD 0A7D7F1F 063B7C82 EA8DCC44 170B1411 CA9ED66F


OtherInfo is
```

```
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         CDFB1507 E397D3DB 9217ABA3 45EF658D
        265DBD98 28F2A91E 6A30EF59 5B099319 E1884D73 E73417BD
        F72451F8 AC4618D2 2232F3C7 F9EC13AB 69AF1F4C 385827BF
        498B2248 63A63612 E1860590 3ADB7F12 AE4B96B2 A7F61FDA
        D963A733 D9B1CF4D C8A4EA1E B2827485 B0EE36F6 BF54D63B
        299190DA 6C2860F5 39B3E0F9 75C801D3 C621A0A3 816E2AFD
        683C91FA 744EACBC 51D0BB2D 17E32286 9C3465CA 3E1577F8


MacData is
                         4B435F31 5F55414C 49434542 4F424259
        077192C3 24FDDF48 74D8B788 244F004F 30FD9A85 9CDB919E
        97CFAE95 16A2703B 56B1EDB8 8D53C17E 3F1A0F4B AF21DA3B
        8ED082BD FE53ACEF F6BB4DE6 93DD4209 DD2D1289 1B594C4C
        05D56CA3 56C46D67 2E8A73CD D02164B7 7A3C54CC 1306B270
        00C70545 3F56BB41 4B191BA3 AE3E2FC1 85AFF2A7 873354DE
        60A21538 039460C3 82456E4C 04FECE44 289F1DFD FE6FB4DE
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB80 87548FEE 838A8607 7AFC2DC3
        D5FBFA15 9E92BCE2 5CDE8DE2 624D9002 0AF07F1F 9730194E


MacKey is
                                                 CDFB1507 E397D3DB
        9217ABA3 45EF658D 265DBD98 28F2A91E 6A30EF59 5B099319


Mtag is
                         F88F2F43 27DCB272 30831872 360CB97B
        A9C8478E F79E3107 6222A992 F7E56A59 6E32B0E7 176FE898
        314FD482 70433157 6CE13931 0BC8050D 28181450 F4D6799E


KeyData is
                                                 E1884D73 E73417BD
        F72451F8 AC4618D2 2232F3C7 F9EC13AB 69AF1F4C 385827BF
        498B2248 63A63612 E1860590 3ADB7F12 AE4B96B2 A7F61FDA
        D963A733 D9B1CF4D C8A4EA1E B2827485 B0EE36F6 BF54D63B
        299190DA 6C2860F5 39B3E0F9 75C801D3 C621A0A3 816E2AFD
        683C91FA 744EACBC 51D0BB2D 17E32286 9C3465CA 3E1577F8
```

Scheme Responder, Key Confirmation Provider: V to U
NonceU is
0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
F19737D1 F8452AC5 54BEEB80 87548FEE 838A8607 7AFC2DC3
D5FBFA15 9E92BCE2 5CDE8DE2 624D9002 0AF07F1F 9730194E

Z is
0050180B DA7D8F75 08DC8D59 6D74136E 961CF6E4 FF2AC680
468A9886 E4F65408 3CD006A1 3BE0FD6E 88BAB1D3 C6DF2375
E1C08BBD 0A7D7F1F 063B7C82 EA8DCC44 170B1411 CA9ED66F

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
CDFB1507 E397D3DB 9217ABA3 45EF658D
265DBD98 28F2A91E 6A30EF59 5B099319 E1884D73 E73417BD
F72451F8 AC4618D2 2232F3C7 F9EC13AB 69AF1F4C 385827BF
498B2248 63A63612 E1860590 3ADB7F12 AE4B96B2 A7F61FDA
D963A733 D9B1CF4D C8A4EA1E B2827485 B0EE36F6 BF54D63B
299190DA 6C2860F5 39B3E0F9 75C801D3 C621A0A3 816E2AFD
683C91FA 744EACBC 51D0BB2D 17E32286 9C3465CA 3E1577F8

MacData is
4B435F31 5F56424F 42425941 4C494345
077192C3 24FDDF48 74D8B788 244F004F 30FD9A85 9CDB919E
97CFAE95 16A2703B 56B1EDB8 8D53C17E 3F1A0F4B AF21DA3B
8ED082BD FE53ACEF F6BB4DE6 93DD4209 DD2D1289 1B594C4C
05D56CA3 56C46D67 2E8A73CD D02164B7 7A3C54CC 1306B270
00C70545 3F56BB41 4B191BA3 AE3E2FC1 85AFF2A7 873354DE
60A21538 039460C3 82456E4C 04FECE44 289F1DFD FE6FB4DE

MacKey is
CDFB1507 E397D3DB
9217ABA3 45EF658D 265DBD98 28F2A91E 6A30EF59 5B099319

Mtag is

```
                        F00A35F1 8687C55C 5CACD6C7 EC24E22A
        45194771 990ECC57 3316BC2C 81B7C036 F87EE843 4228B256
        626B4356 1247C981 ADD5BE69 B0AE70B6 933A8988 A7F423FA


KeyData is
                                                E1884D73 E73417BD
        F72451F8 AC4618D2 2232F3C7 F9EC13AB 69AF1F4C 385827BF
        498B2248 63A63612 E1860590 3ADB7F12 AE4B96B2 A7F61FDA
        D963A733 D9B1CF4D C8A4EA1E B2827485 B0EE36F6 BF54D63B
        299190DA 6C2860F5 39B3E0F9 75C801D3 C621A0A3 816E2AFD
        683C91FA 744EACBC 51D0BB2D 17E32286 9C3465CA 3E1577F8




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB80 87548FEE 838A8607 7AFC2DC3
        D5FBFA15 9E92BCE2 5CDE8DE2 624D9002 0AF07F1F 9730194E


Z is
        0050180B DA7D8F75 08DC8D59 6D74136E 961CF6E4 FF2AC680
        468A9886 E4F65408 3CD006A1 3BE0FD6E 88BAB1D3 C6DF2375
        E1C08BBD 0A7D7F1F 063B7C82 EA8DCC44 170B1411 CA9ED66F


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                        CDFB1507 E397D3DB 9217ABA3 45EF658D
        265DBD98 28F2A91E 6A30EF59 5B099319 E1884D73 E73417BD
        F72451F8 AC4618D2 2232F3C7 F9EC13AB 69AF1F4C 385827BF
        498B2248 63A63612 E1860590 3ADB7F12 AE4B96B2 A7F61FDA
        D963A733 D9B1CF4D C8A4EA1E B2827485 B0EE36F6 BF54D63B
        299190DA 6C2860F5 39B3E0F9 75C801D3 C621A0A3 816E2AFD
        683C91FA 744EACBC 51D0BB2D 17E32286 9C3465CA 3E1577F8


U2V
----------------
```

```
MacData is
                        4B435F32 5F55414C 49434542 4F424259
        077192C3 24FDDF48 74D8B788 244F004F 30FD9A85 9CDB919E
        97CFAE95 16A2703B 56B1EDB8 8D53C17E 3F1A0F4B AF21DA3B
        8ED082BD FE53ACEF F6BB4DE6 93DD4209 DD2D1289 1B594C4C
        05D56CA3 56C46D67 2E8A73CD D02164B7 7A3C54CC 1306B270
        00C70545 3F56BB41 4B191BA3 AE3E2FC1 85AFF2A7 873354DE
        60A21538 039460C3 82456E4C 04FECE44 289F1DFD FE6FB4DE
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB80 87548FEE 838A8607 7AFC2DC3
        D5FBFA15 9E92BCE2 5CDE8DE2 624D9002 0AF07F1F 9730194E


MacKey is
                                                CDFB1507 E397D3DB
        9217ABA3 45EF658D 265DBD98 28F2A91E 6A30EF59 5B099319


Mtag is
                        950C34D9 0DC0DF60 4D3F6317 34E24B0E
        4D0C46CF 15810C3A 3438888E 8CA415F7 4F081F4A EAEECB52
        644237D8 68001C4C 4DD70552 41E9C5C3 AC482825 9A9BF1F7


V2U
----------------
MacData is
                        4B435F32 5F56424F 42425941 4C494345
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB80 87548FEE 838A8607 7AFC2DC3
        D5FBFA15 9E92BCE2 5CDE8DE2 624D9002 0AF07F1F 9730194E
        077192C3 24FDDF48 74D8B788 244F004F 30FD9A85 9CDB919E
        97CFAE95 16A2703B 56B1EDB8 8D53C17E 3F1A0F4B AF21DA3B
        8ED082BD FE53ACEF F6BB4DE6 93DD4209 DD2D1289 1B594C4C
        05D56CA3 56C46D67 2E8A73CD D02164B7 7A3C54CC 1306B270
        00C70545 3F56BB41 4B191BA3 AE3E2FC1 85AFF2A7 873354DE
        60A21538 039460C3 82456E4C 04FECE44 289F1DFD FE6FB4DE


MacKey is
                                                CDFB1507 E397D3DB
        9217ABA3 45EF658D 265DBD98 28F2A91E 6A30EF59 5B099319


Mtag is
                        3D33BEDF 057EC698 7C4C9A45 44CB3862
```

```
        CB526A78 E2F52E5F 68EA4736 F651B6BC 4F0CC2CF 7A248278
        320ADCD2 662E61D5 8DC683F3 CEBEBCAB ED5A6155 A11DBB19


KeyData is
                                            E1884D73 E73417BD
        F72451F8 AC4618D2 2232F3C7 F9EC13AB 69AF1F4C 385827BF
        498B2248 63A63612 E1860590 3ADB7F12 AE4B96B2 A7F61FDA
        D963A733 D9B1CF4D C8A4EA1E B2827485 B0EE36F6 BF54D63B
        299190DA 6C2860F5 39B3E0F9 75C801D3 C621A0A3 816E2AFD
        683C91FA 744EACBC 51D0BB2D 17E32286 9C3465CA 3E1577F8




OnePassDiffieHellmanCDH(B-571)
------------------------------------------------------------
dsV is
        01823854 AF10876C 19AEE8EC 6691AD9E 7E294860 5347F7DF
        0EB770FE EB2E71B9 8FAB3273 F7DB3994 AE86986A 7D5533F3
        7556EE07 7B1F9270 A1B990CA 10296BA3 7632CD9F D2F43B6B


QsV_x is
        0431E29F 977CDEA2 90E063C8 3F6B4A0D E33D083C C1844BC4
        60303F63 53FB2B86 888C1BA7 81F89A6E FFA2447C F1E4E772
        E77E8FF6 3243DE77 1692EB0B AE333456 8CF11AE0 9422916F


QsV_y is
        01530D05 C336B8C0 121149A2 3416951E D557A58E 4F2A6F64
        3CFBA1F1 D508C329 100302D2 BB783676 E0AECE33 EBA2FBFC
        8057E158 D9447DC6 D6BF523D 3077CAB6 9590871E C80155B1


deU is
        013AC597 40DDBC84 E4803312 4D269467 71CC4872 706EF9F6
        34CE0E8A F1A227E8 E14A0898 53A989E5 BE24D464 0D4D6947
        884A7936 2618DA2A 14AC7EEB 06DC5BEE C9775477 444EA803


QeU_x is
        077192C3 24FDDF48 74D8B788 244F004F 30FD9A85 9CDB919E
        97CFAE95 16A2703B 56B1EDB8 8D53C17E 3F1A0F4B AF21DA3B
        8ED082BD FE53ACEF F6BB4DE6 93DD4209 DD2D1289 1B594C4C
```

```
QeU_y is
        05D56CA3 56C46D67 2E8A73CD D02164B7 7A3C54CC 1306B270
        00C70545 3F56BB41 4B191BA3 AE3E2FC1 85AFF2A7 873354DE
        60A21538 039460C3 82456E4C 04FECE44 289F1DFD FE6FB4DE




------------------------------------------------------------
no Key Confirmation
Z is
        07C93A62 8305A453 88803054 2685F73A 273F5245 B9591F45
        1C3BC32B 35135F14 C00E22A4 C10017A0 D67EC191 5267516E
        E70DCFCB 7DD9748B E73B06AA BD5F6662 4D6B1A8F 84CA2572


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                            34B51BC2 5FF54279
        1B532B36 EE0695D5 A64B8868 39953553 AAF4A5BA D406A39E
        989CB0C8 2BE4E1A0 0D1D29E3 A784481A 712DB2F8 542E27F7
        98239909 E0657239 8A84DD99 FD0356C0 0478A260 7266CB94
        882906DD 52C56FBA 2BA9742B 8007A7D6 48CCF207 3A99BBE7
        73DEE92E A1942C51 4DE1B4BC E39A53D4 BA655BB3 A5CBD5FA


KeyData is
                                            34B51BC2 5FF54279
        1B532B36 EE0695D5 A64B8868 39953553 AAF4A5BA D406A39E
        989CB0C8 2BE4E1A0 0D1D29E3 A784481A 712DB2F8 542E27F7
        98239909 E0657239 8A84DD99 FD0356C0 0478A260 7266CB94
        882906DD 52C56FBA 2BA9742B 8007A7D6 48CCF207 3A99BBE7
        73DEE92E A1942C51 4DE1B4BC E39A53D4 BA655BB3 A5CBD5FA




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
        07C93A62 8305A453 88803054 2685F73A 273F5245 B9591F45
        1C3BC32B 35135F14 C00E22A4 C10017A0 D67EC191 5267516E
```

```
        E70DCFCB 7DD9748B E73B06AA BD5F6662 4D6B1A8F 84CA2572


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         34B51BC2 5FF54279 1B532B36 EE0695D5
        A64B8868 39953553 AAF4A5BA D406A39E 989CB0C8 2BE4E1A0
        0D1D29E3 A784481A 712DB2F8 542E27F7 98239909 E0657239
        8A84DD99 FD0356C0 0478A260 7266CB94 882906DD 52C56FBA
        2BA9742B 8007A7D6 48CCF207 3A99BBE7 73DEE92E A1942C51
        4DE1B4BC E39A53D4 BA655BB3 A5CBD5FA 638F61B8 C5C4A119
        1665CC23 50F3E2F2 C2D650BA D71AC3BE 505B3023 7447DE17


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        077192C3 24FDDF48 74D8B788 244F004F 30FD9A85 9CDB919E
        97CFAE95 16A2703B 56B1EDB8 8D53C17E 3F1A0F4B AF21DA3B
        8ED082BD FE53ACEF F6BB4DE6 93DD4209 DD2D1289 1B594C4C
        05D56CA3 56C46D67 2E8A73CD D02164B7 7A3C54CC 1306B270
        00C70545 3F56BB41 4B191BA3 AE3E2FC1 85AFF2A7 873354DE
        60A21538 039460C3 82456E4C 04FECE44 289F1DFD FE6FB4DE


MacKey is
                                            34B51BC2 5FF54279
        1B532B36 EE0695D5 A64B8868 39953553 AAF4A5BA D406A39E


Mtag is
                         D760F0D6 4520DB78 84CF0509 17DD3881
        885927A4 018259B4 4EDCA214 C27DA29C D5D18398 6616162A
        E560BE4E 025D4F66 786A3A99 C853CF1A 0E4C5816 EF806E1E


KeyData is
                                            989CB0C8 2BE4E1A0
        0D1D29E3 A784481A 712DB2F8 542E27F7 98239909 E0657239
        8A84DD99 FD0356C0 0478A260 7266CB94 882906DD 52C56FBA
        2BA9742B 8007A7D6 48CCF207 3A99BBE7 73DEE92E A1942C51
        4DE1B4BC E39A53D4 BA655BB3 A5CBD5FA 638F61B8 C5C4A119
        1665CC23 50F3E2F2 C2D650BA D71AC3BE 505B3023 7447DE17
```

StaticUnifiedCDH(B-571)
---
dsU is
009B592D 32F99420 05A38021 D26E7AA6 ED3E78BB DFF2A861
311B89C9 9DF67762 8EE47F3D 7A6FA271 9B746E08 B842A86C
DBA72250 A188351F 37229380 29EFE9C9 74DF46DD 01CF49F7

QsU_x is
06A2D2E1 0ECAB26F 84010BC7 05D733EF BEBDDEC1 E2010EDA
B7CF1CED 6CDD9F2C CE111C6D D8271ACA 6046A189 F332BC40
C602A93C 4F3F67D3 79E369C5 E842E2E3 0603FC56 2F72E21F

QsU_y is
0439C4DC 44E29DF3 BBAC9EA3 4370856F 3F733641 1D9AD09E
8FA92D74 27F2FD12 13F7F17E 0DAFA972 93A50076 41240A9F
2A45059E CB0ABC4B 18916C18 663104CC 059F457B 1EFA7FA0

dsV is
01823854 AF10876C 19AEE8EC 6691AD9E 7E294860 5347F7DF
0EB770FE EB2E71B9 8FAB3270 F7DD39B4 BC0A96CB 7D4437F2
71C7CDC7 7E9302B1 A1FB90E0 1EA179B3 E612C585 D2F4334B

QsV_x is
01FFAD44 91BF3C68 FFB1F0F6 9C89FAE5 0F38D47F 99E0AFE8
FAF77589 EB6931FE 8947C149 6E73BA63 EE3E28A0 917F4FFE
F76676AE 16027F2A 4DE3D6C4 DEAB9FE2 8E48D252 7922526A

QsV_y is
01088E7E 80C3E7D3 63F5AC7D D601E11D 0738F329 4AA308F5
8A4E0A21 916BC74A 6FBF379C 76A03E4F 21CB4B24 615962C6
2CB51EED EA996040 06024312 432DE145 59016BEE C44E1271

---
no Key Confirmation
NonceU is

```
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB80 87548FEE 838A8607 7AFC2DC3
        D5FBFA15 9E92BCE2 5CDE8DE2 624D9002 0AF07F1F 9730194E


Z is
        04C19ADE F0359BFC 001AA49A 6EBE9779 DCF4EB3B 7CF2AF26
        273D1DC9 EDD7CFA2 1107B593 26D651EF 19FF8957 79C30F95
        9924E3FF 1D8D14AE 6201D453 83E45552 515CCCA3 5DED0505


OtherInfo is
                                                          1234
        56789ABC DEF0414C 49434531 32333B02 0051D0BA 0638CE20
        905F7F3A 0298275E 33482000 1D90F0B2 F19737D1 F8452AC5
        54BEEB80 87548FEE 838A8607 7AFC2DC3 D5FBFA15 9E92BCE2
        5CDE8DE2 624D9002 0AF07F1F 9730194E 424F4242 59343536


DerivedKeyMaterial is
                                            3291B29A 8308E02F
        D7CDAC4D 7B1A3F8A 19792B8D 395BEFD4 98695E43 0ACD68D6
        7577239D 2FE314B8 67BE58C0 067F9948 C43C47C9 40540D2B
        52316A75 075684D4 FE1CEC88 2A2B1232 DC910D02 02D0213B
        7571F930 70FC6B9E 0B28BAD4 CD0E6793 62AA0179 B4031BD9
        EBED5420 1DDBFD37 25E24C36 E62CA373 C3B71FBF 3CE3DEA4


KeyData is
                                            3291B29A 8308E02F
        D7CDAC4D 7B1A3F8A 19792B8D 395BEFD4 98695E43 0ACD68D6
        7577239D 2FE314B8 67BE58C0 067F9948 C43C47C9 40540D2B
        52316A75 075684D4 FE1CEC88 2A2B1232 DC910D02 02D0213B
        7571F930 70FC6B9E 0B28BAD4 CD0E6793 62AA0179 B4031BD9
        EBED5420 1DDBFD37 25E24C36 E62CA373 C3B71FBF 3CE3DEA4




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceU is
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB80 87548FEE 838A8607 7AFC2DC3
        D5FBFA15 9E92BCE2 5CDE8DE2 624D9002 0AF07F1F 9730194E
```

NonceV is
        00A05A4D DA59C82A 26EAF7F8 44D4C41E 622F4AA9 17AB5F06
        5A452352 1700C41A 5234B398 D09E8790 08E55746 AF7D6C15
        10EAB743 B1DEDE78 BF0FAF60 53B98ABA 894B0937 C7200118

Z is
        04C19ADE F0359BFC 001AA49A 6EBE9779 DCF4EB3B 7CF2AF26
        273D1DC9 EDD7CFA2 1107B593 26D651EF 19FF8957 79C30F95
        9924E3FF 1D8D14AE 6201D453 83E45552 515CCCA3 5DED0505

OtherInfo is
                                                            1234
        56789ABC DEF0414C 49434531 32333B02 0051D0BA 0638CE20
        905F7F3A 0298275E 33482000 1D90F0B2 F19737D1 F8452AC5
        54BEEB80 87548FEE 838A8607 7AFC2DC3 D5FBFA15 9E92BCE2
        5CDE8DE2 624D9002 0AF07F1F 9730194E 424F4242 59343536

DerivedKeyMaterial is
                          3291B29A 8308E02F D7CDAC4D 7B1A3F8A
        19792B8D 395BEFD4 98695E43 0ACD68D6 7577239D 2FE314B8
        67BE58C0 067F9948 C43C47C9 40540D2B 52316A75 075684D4
        FE1CEC88 2A2B1232 DC910D02 02D0213B 7571F930 70FC6B9E
        0B28BAD4 CD0E6793 62AA0179 B4031BD9 EBED5420 1DDBFD37
        25E24C36 E62CA373 C3B71FBF 3CE3DEA4 FA135517 C337829F
        74B77E25 9266B9A5 048864C3 153303CE 6D100BAF 2CFC2CC5

MacData is
                          4B435F31 5F55414C 49434542 4F424259
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB80 87548FEE 838A8607 7AFC2DC3
        D5FBFA15 9E92BCE2 5CDE8DE2 624D9002 0AF07F1F 9730194E
        00A05A4D DA59C82A 26EAF7F8 44D4C41E 622F4AA9 17AB5F06
        5A452352 1700C41A 5234B398 D09E8790 08E55746 AF7D6C15
        10EAB743 B1DEDE78 BF0FAF60 53B98ABA 894B0937 C7200118

MacKey is
                                                  3291B29A 8308E02F
        D7CDAC4D 7B1A3F8A 19792B8D 395BEFD4 98695E43 0ACD68D6

Mtag is
                        81C845D7 CA7C7D8E 4F35E6C4 F4C31221
        F9354D52 90527E74 0F05A101 E47215BF C6B7672D 09DD8E89
        3BB8BF5B 23AFC490 73953885 3DA7B27C 83F1377D 9FC5F8E4

KeyData is
                                                7577239D 2FE314B8
        67BE58C0 067F9948 C43C47C9 40540D2B 52316A75 075684D4
        FE1CEC88 2A2B1232 DC910D02 02D0213B 7571F930 70FC6B9E
        0B28BAD4 CD0E6793 62AA0179 B4031BD9 EBED5420 1DDBFD37
        25E24C36 E62CA373 C3B71FBF 3CE3DEA4 FA135517 C337829F
        74B77E25 9266B9A5 048864C3 153303CE 6D100BAF 2CFC2CC5

Scheme Responder, Key Confirmation Provider: V to U
NonceV is
        00A05A4D DA59C82A 26EAF7F8 44D4C41E 622F4AA9 17AB5F06
        5A452352 1700C41A 5234B398 D09E8790 08E55746 AF7D6C15
        10EAB743 B1DEDE78 BF0FAF60 53B98ABA 894B0937 C7200118

NonceU is
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB80 87548FEE 838A8607 7AFC2DC3
        D5FBFA15 9E92BCE2 5CDE8DE2 624D9002 0AF07F1F 9730194E

Z is
        04C19ADE F0359BFC 001AA49A 6EBE9779 DCF4EB3B 7CF2AF26
        273D1DC9 EDD7CFA2 1107B593 26D651EF 19FF8957 79C30F95
        9924E3FF 1D8D14AE 6201D453 83E45552 515CCCA3 5DED0505

OtherInfo is
                                                          1234
        56789ABC DEF0414C 49434531 32333B02 0051D0BA 0638CE20
        905F7F3A 0298275E 33482000 1D90F0B2 F19737D1 F8452AC5
        54BEEB80 87548FEE 838A8607 7AFC2DC3 D5FBFA15 9E92BCE2
        5CDE8DE2 624D9002 0AF07F1F 9730194E 424F4242 59343536

DerivedKeyMaterial is

```
                        3291B29A 8308E02F D7CDAC4D 7B1A3F8A
        19792B8D 395BEFD4 98695E43 0ACD68D6 7577239D 2FE314B8
        67BE58C0 067F9948 C43C47C9 40540D2B 52316A75 075684D4
        FE1CEC88 2A2B1232 DC910D02 02D0213B 7571F930 70FC6B9E
        0B28BAD4 CD0E6793 62AA0179 B4031BD9 EBED5420 1DDBFD37
        25E24C36 E62CA373 C3B71FBF 3CE3DEA4 FA135517 C337829F
        74B77E25 9266B9A5 048864C3 153303CE 6D100BAF 2CFC2CC5


MacData is
                        4B435F31 5F56424F 42425941 4C494345
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB80 87548FEE 838A8607 7AFC2DC3
        D5FBFA15 9E92BCE2 5CDE8DE2 624D9002 0AF07F1F 9730194E


MacKey is
                                                3291B29A 8308E02F
        D7CDAC4D 7B1A3F8A 19792B8D 395BEFD4 98695E43 0ACD68D6


Mtag is
                        956C0D92 4608AE48 31B6535D 33544C81
        25E07CA5 9E6B5CB5 573C36CB 2474ACB7 0DA01475 3EA13E6B
        AA3EDFEC B5017A30 6AA2766B 99227A52 F9927C5F FD28C2E7


KeyData is
                                                7577239D 2FE314B8
        67BE58C0 067F9948 C43C47C9 40540D2B 52316A75 075684D4
        FE1CEC88 2A2B1232 DC910D02 02D0213B 7571F930 70FC6B9E
        0B28BAD4 CD0E6793 62AA0179 B4031BD9 EBED5420 1DDBFD37
        25E24C36 E62CA373 C3B71FBF 3CE3DEA4 FA135517 C337829F
        74B77E25 9266B9A5 048864C3 153303CE 6D100BAF 2CFC2CC5




------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
NonceU is
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB80 87548FEE 838A8607 7AFC2DC3
        D5FBFA15 9E92BCE2 5CDE8DE2 624D9002 0AF07F1F 9730194E
```

```
NonceV is
        00A05A4D DA59C82A 26EAF7F8 44D4C41E 622F4AA9 17AB5F06
        5A452352 1700C41A 5234B398 D09E8790 08E55746 AF7D6C15
        10EAB743 B1DEDE78 BF0FAF60 53B98ABA 894B0937 C7200118


Z is
        04C19ADE F0359BFC 001AA49A 6EBE9779 DCF4EB3B 7CF2AF26
        273D1DC9 EDD7CFA2 1107B593 26D651EF 19FF8957 79C30F95
        9924E3FF 1D8D14AE 6201D453 83E45552 515CCCA3 5DED0505


OtherInfo is
                                                          1234
        56789ABC DEF0414C 49434531 32333B02 0051D0BA 0638CE20
        905F7F3A 0298275E 33482000 1D90F0B2 F19737D1 F8452AC5
        54BEEB80 87548FEE 838A8607 7AFC2DC3 D5FBFA15 9E92BCE2
        5CDE8DE2 624D9002 0AF07F1F 9730194E 424F4242 59343536


DerivedKeyMaterial is
                         3291B29A 8308E02F D7CDAC4D 7B1A3F8A
        19792B8D 395BEFD4 98695E43 0ACD68D6 7577239D 2FE314B8
        67BE58C0 067F9948 C43C47C9 40540D2B 52316A75 075684D4
        FE1CEC88 2A2B1232 DC910D02 02D0213B 7571F930 70FC6B9E
        0B28BAD4 CD0E6793 62AA0179 B4031BD9 EBED5420 1DDBFD37
        25E24C36 E62CA373 C3B71FBF 3CE3DEA4 FA135517 C337829F
        74B77E25 9266B9A5 048864C3 153303CE 6D100BAF 2CFC2CC5


U2V
----------------
MacData is
                         4B435F32 5F55414C 49434542 4F424259
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB80 87548FEE 838A8607 7AFC2DC3
        D5FBFA15 9E92BCE2 5CDE8DE2 624D9002 0AF07F1F 9730194E
        00A05A4D DA59C82A 26EAF7F8 44D4C41E 622F4AA9 17AB5F06
        5A452352 1700C41A 5234B398 D09E8790 08E55746 AF7D6C15
        10EAB743 B1DEDE78 BF0FAF60 53B98ABA 894B0937 C7200118


MacKey is
                                                  3291B29A 8308E02F
        D7CDAC4D 7B1A3F8A 19792B8D 395BEFD4 98695E43 0ACD68D6
```

```
Mtag is
                        3A64F3E9 EE792D00 1E5874DF 82FC10BC
        40D17F5D 5D7D6843 FD4065B1 B1FB740D 7A6B43A3 75D5D67C
        1C0031F5 B2A7D530 A25179F5 19D3E229 6C261384 7B423C0A


V2U
----------------
MacData is
                        4B435F32 5F56424F 42425941 4C494345
        00A05A4D DA59C82A 26EAF7F8 44D4C41E 622F4AA9 17AB5F06
        5A452352 1700C41A 5234B398 D09E8790 08E55746 AF7D6C15
        10EAB743 B1DEDE78 BF0FAF60 53B98ABA 894B0937 C7200118
        0051D0BA 0638CE20 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB80 87548FEE 838A8607 7AFC2DC3
        D5FBFA15 9E92BCE2 5CDE8DE2 624D9002 0AF07F1F 9730194E


MacKey is
                                                3291B29A 8308E02F
        D7CDAC4D 7B1A3F8A 19792B8D 395BEFD4 98695E43 0ACD68D6


Mtag is
                        1ED8CF3A 9453A076 25337F43 0B121D3F
        4660E2D0 6B1694CC 2AFC7226 475500D5 AF7BEB9A 4ABD1E6D
        7348DE57 051AEC8C 1F8C565F 7F7CC62B AAF86755 A9791382


KeyData is
                                                7577239D 2FE314B8
        67BE58C0 067F9948 C43C47C9 40540D2B 52316A75 075684D4
        FE1CEC88 2A2B1232 DC910D02 02D0213B 7571F930 70FC6B9E
        0B28BAD4 CD0E6793 62AA0179 B4031BD9 EBED5420 1DDBFD37
        25E24C36 E62CA373 C3B71FBF 3CE3DEA4 FA135517 C337829F
        74B77E25 9266B9A5 048864C3 153303CE 6D100BAF 2CFC2CC5
```