System Infrastructure Provider to FPKI Shared Service Provider Interface Specification

Version 1.0.0

February 7, 2007

hspd12

Document History

Status	Release	Date	Comment	Audience
Draft	0.0.1	11/08/06	Initial Document Creation	AWG
Draft	0.0.2	11/14/06	Formatting changes, clarifications	AWG
Draft	0.0.3	11/20/06	Added certificate revocation/suspension, formatting changes,UPN attribute added	AWG
Draft	0.0.4	12/05/06	Added certificate un-suspension, re-key, and update	AWG
Draft	0.0.5	12/13/06	Final internal review	Enspier
Draft	0.1.0	12/15/06	Released for public review	Public
Final	1.0.0	2/7/07		Public

Editors

Chris Brown	Dave Silver	

Table of Contents

Figures

1 Introduction

This document provides the interface specification for Systems Infrastructure Provider (SIP) and Federal Public Key Infrastructure (FPKI) Shared Service Provider (SSP) data exchange. It is a standard, re-usable shared service specification for Federal government-wide use, per [SCI Architecture]. Therefore, one should read [SCI Architecture] before reading this specification.

The following transactions only pertain to obtaining the Personal Identity Verification (PIV) authentication certificate that corresponds to the PIV authentication asymmetric private key mandated by [FIPS201]. The optional PIV digital signature key and PIV key management key are not included in this specification.

This interface specification scopes the Certificate Management Protocol (CMP) defined in [RFC 4210]. CMP is an ASN.1 based protocol that defines common PKI management functions. CMP is composed of three data structures: PKIHeader, PKIBody, and Protection. The PKIHeader contains transaction information and security information. The PKIBody contains the Public Key Infrastructure (PKI) management function that is being performed. The Protection field contains the bits of the digital signature used to protect the message. It is assumed that all keywords (e.g., MUST) contained within [RFC 4210] are followed, and therefore are not mentioned in this document. The following PKI management functions are addressed in this profile:

- Initial Certificate Issuance
- Revocation
- Suspension
- Un-Suspension
- Re-key
- Update

All CMP messages are transported over HTTPS. Once the Transport Layer Security (TLS) session has been established, communication proceeds as defined in [CMP-Transport], Section 4. FPKI SSPs shall publish a URL, via a metadata file, where authorized SIPs initiate a TLS session. The metadata will also contain a unique SCI identifier assigned by the SCI governing authority. All CMP requests and responses are digitally signed via the Protection structure contained within the CMP.

This document does not supersede or contradict any existing National Institute of Standards and Technology (NIST) publication, and should be used in conjunction with existing policies and procedures.

1.1 Authority

This document has been developed on behalf of The Office of Governmentwide Policy and the HSPD-12 Executive Steering Committee in furtherance of their charter to implement HSPD-12 from a “national” perspective.

1.2 References

[CMP-Transport] Transport Protocols for CMP
http://tools.ietf.org/wg/pkix/draft-ietf-pkix-cmp-transport-protocols/draft-ietf-pkix-cmp-transport-protocols-05.txt

[Common Policy] X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework
http://www.cio.gov/ficc/documents/CommonPolicy.pdf

[FIPS 201] FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* NIST, March 2006.
http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

[RFC 4210] Certificate Management Protocol
http://www.ietf.org/rfc/rfc4210.txt

[RFC 4211] Certificate Request Message Format
http://www.ietf.org/rfc/rfc4211.txt

[SCI Architecture] HSPD-12 Shared Component Architecture
http://www.smart.gov/awg/documents/HSPD12sca.pdf

[SCI Interoperability] HSPD-12 Shared Component Infrastructure Technical Interoperability Model
http://www.smart.gov/awg/documents/SCItechnicalIOmodel.pdf

[SCI Trust] HSPD-12 Shared Component Infrastructure Trust Model
http://www.smart.gov/awg/documents/SCItrustModel.pdf

[SP800-78] Cryptographic Algorithms and Key Sizes for PIV
http://csrc.nist.gov/publications/nistpubs/800-78/sp800-78-final.pdf

2 Initial Certificate Issuance

Initial Certificate Issuance consists of four (4) messages between the SIP and FPKI SSP:

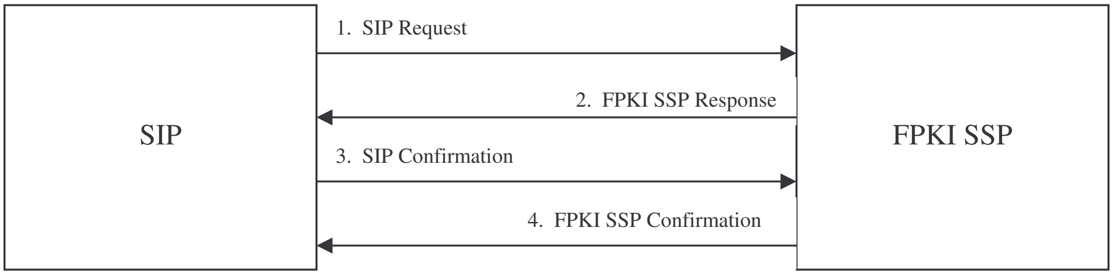
1. Certification request;
2. Certification response;
3. Certification confirmation; and
4. FPKI SSP confirmation

The message flow is as follows:

1. The first message is a request for a PIV authentication certificate from the SIP to the FPKI SSP.
2. If the request was successfully processed, the FPKI SSP sends the SIP a certificate.
3. The SIP sends an acknowledgement (ACK) message to the FPKI SSP. The SIP must accept the returned certificate. The ACK message is sent to the FPKI SSP regardless of whether the SIP accepts or rejects the certificate.
4. The FPKI SSP sends the SIP a confirmation message that it has received the SIP acknowledgement.

Figure 2-1 presents a high-level sequence diagram of the transactions.

Figure 2-1: Transaction Sequence Diagram



The following sections describe fields and constraints of each message.

2.1 SIP Authentication Certificate Request

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
sender	the name identifying the SIP	Required. Data type must be directoryName Value must be the SubjectDN in the SIP SCI Issued Certificate
recipient	the name of the CA who is being asked to produce a certificate	Required. Data type must be directoryName. Use the value of SubjectDN in the CA certificate.
protectionAlg	signature algorithm used to protect this message	Required. MSG_SIG_ALG[1]
senderKID	the reference number which the CA has previously issued to the end entity (together with the MACing key)	Must Not be used
transactionID	unique id sent from the SIP to the FPKI SSP	Required. Combination of SIP unique identifier issued by the SCI Governing Authority plus 20 random bytes.
senderNonce	128 random bits used to protect against replay attacks	Required. 128 Random Bits
freeText	human readable information	Not used
cr.crm[0]	certificate request message structure	Required.
cr.crm[0].certReq.certReqId	index of certificate request messages	Required. Fixed value of 0
cr.crm[0].certReq.certTemplate	describes fields that the SIP wishes to contain in the certificate	Required.
cr.crm[0].certReq.certTemplate.publicKey	subject public key	Required. Must contain the subject public key. [2]

[1] Refer to Appendix B for valid signature algorithm values.

[2] Public key algorithm must be RSA or ECDSA. Refer to [SP800-78] for details.

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
cr.crm[0].certReq.certTemplate.extension.subjectAltName	subject alternative name extension	Required. -Must contain the FASC-N attribute in the subjectAltName extension -Optionally may contain UPN attribute in the subjectAltName extension[3]
cr.crm[0].certReq.certTemplate.extension.NACI	PIV NACI indicator private extension	Required. -Must contain the PIV NACI indicator extension.[4]
cr.crm[0].pop.POPOSigningKey	proof of possession of the private signing key	Required.
cr.crm[0].controls.archiveOptions	a request to the FPKI SSP to archive the end user's private key	Not used. SIP may not archive the private key.
cr.crm[0].certReq.controls.publicationInfo	a request to the FPKI SSP to publish the certificate in a directory server	Optional. SIP may request that the FPKI SSP publishes the certificate
protection	signature of message	Required. Must be calculated according to MSG_SIG_ALG

2.2 FPKI SSP Certificate Response

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
sender	the name of the CA who produced the message	Required. Data type must be directoryName Use the value of SubjectDN in the FPKI SSP CA certificate
recipient	the name of the SIP which requested the certificate	Required. Data type must be directoryName. Value must be the SubjectDN in the SIP SCI Trust Certificate.
messageTime	time at which the CA produced the message	Required

[3] The UPN will help facilitate network login and provisioning to active directory. Implementers must use otherName attribute using "1.3.6.1.4.1.311.20.2.3" as the oid value.

[4] FIPS 201 Appendix D.2

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
protectectionAlg	signature algorithm used to protect this message	Required. MSG_SIG_ALG[5]
senderKID	the reference number which the CA has previously issued to the end entity (together with the MACing key)	Must not be used
transactionID	value from corresponding request message	Required. Use corresponding value from SIP Authentication Certificate Request.
senderNonce	128 random bits used to protect against replay attacks	Required.
recipNonce	128 random bits used to protect against replay attacks	Required. Value from senderNonce from certificate response message.
freeText	human readable information	Optional. Values may be: "<CA> successfully received certificate request"
cp.crc	certificate reply structure	Required.
cp.crc[0].certReqId	request id that corresponds to the request in the certificate request message	Required. fixed value of zero
cp.crc[0].status.status	status message	Required. Values may be: "accepted" "rejection"
cp.crc[0].status.failInfo	message explaining why certificate generation failed	Optional. Use only if crc[0].status.status = "rejection"
cp.crc[0].certifiedKeyPair	structure that contains the certificate	Required if certificate request was accepted
cp.crc[0].certifiedKeyPair.certificate	certificate	Required
cp.crc[0].certifiedKeyPair.encryptedCert	encryption certificate	Must not be used
cp.crc[0].certifiedKeyPair.publicationInfo	indicates where the certificate has been published	Optional. Present only if SIP requests that the certificate is published
protection	signature of message	Required. Must be calculated according to

[5] Refer to Appendix B for valid signature algorithm values.

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
		MSG_SIG_ALG.
extraCerts	additional certificates	Optional. The FPKI SSP may provide extra certificates that would facilitate path validation.

2.3 SIP Certificate confirmation

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
sender	the name of the CA who produced the message	Required. Data type must be directoryName. Value must be the SubjectDN in the SIP SCI Issued Certificate.
recipient	the name of the CA who is being asked to produce a certificate	Required. Data type must be directoryName. Use the value of SubjectDN in the CA certificate.
transactionID	transaction ID	Required. Value from corresponding initialization request/response
senderNonce	128 random bits used to protect against replay attacks	Required.
recipNonce	128 random bits used to protect against replay attacks	Required. Value from senderNonce from certificate request message.
protectionAlg	signature algorithm used to protect this message	Required. MSG_SIG_ALG[6]
senderKID	the reference number which the CA has previously issued to the end entity (together with the MACing key)	Must not be used.
certConf.ccc[0]	certificate confirm content data structure	Optional. This data structure is only present if the returned certificate from the FPKI SSP is accepted.
certConf.ccc[0].certHash	a hash value of the certificate	Required. Value must be sha-1 hash of the certificate returned by the FPKI SSP.

[6] Refer to Appendix B for valid signature algorithm values.

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
certConf.ccc[0].certReqId	request id that corresponds to the certificate request	Required. Fixed value of 0.
certConf.ccc[0].statusInfo	status info regarding acceptance of certificate	Must not be used.
protection	signature of message	Required. Must be calculated according to MSG_SIG_ALG

2.4 FPKI SSP Confirmation

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
sender	the name of the CA who produced the message	Required. Data type must be directoryName Value must be the SubjectDN in the FPKI SSP CA certificate.
recipient	the name of the SIP which requested the certificate	Required. Data type must be directoryName Value must be the SubjectDN in the SIP SCI Issued Certificate.
transactionID	transaction ID	Required.
senderNonce	128 random bits used to protect against replay attacks	Required.
recipNonce	128 random bits used to protect against replay attacks	Required. Value from senderNonce from certificate confirmation message.
protectionAlg	signature algorithm used to protect this message	Required. MSG_SIG_ALG[7]
senderKID	the reference number which the CA has previously issued to the end entity (together with the MACing key)	Must not be used.
pkiConf	PKI confirmation message	Required. The value is always NULL.
protection	signature of message	Required. Must be calculated according to MSG_SIG_ALG

[7] Refer to Appendix B for valid signature algorithm values.

3 PIV Authentication Certificate Revocation

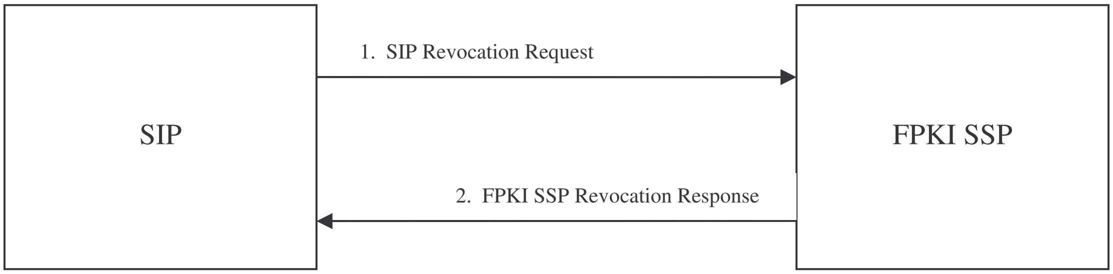
[SCI Architecture] requires a SIP to request a revocation of an FPKI SSP issued certificate on behalf of the end user. The transaction consists of two (2) messages between the SIP and FPKI SSP:

1. SIP revocation request; and
2. FPKI SSP revocation response

A SIP MUST NOT request that more than one certificate is revoked in one SIP revocation request.

Figure 3-1 presents a high-level sequence diagram of the transactions.

Figure 3-1: Transaction Sequence Diagram



3.1 SIP Revocation Request

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
sender	the name identifying the SIP	Required. Value must be the SubjectDN in the SIP SCI Issued Certificate
recipient	the name of the CA who is being asked to produce a certificate	Required. Data type must be directoryName. Use the value of SubjectDN in the FPKI SSP CA certificate.
protectionAlg	signature algorithm used to protect this message	Required. MSG_SIG_ALG[8]
senderKID	the reference number which the CA has previously issued to the end entity (together with the MACing key)	Must Not be used
transactionID	unique id sent from the SIP to the FPKI SSP	Required. Combination of SIP unique identifier issued by the SCI governing Authority plus 20 random bytes.
senderNonce	128 random bits used to protect against replay attacks	Required. 128 Random Bits
freeText	human readable information	Must not be used
rrc	revocation request content structure	Required.
rrc.certDetails.serialNumber	uniquely identifies the end certificate	Required. The SIP may include other fields in the certificate template such as subject
rrc.crlEntryDetails.reasonCode	the reasonCode is a non-critical CRL entry extension that identifies the reason for the certificate revocation	Optional. The SIP may include a valid reason code.
rrc.crlEntryDetails.holdInstructionCode	indicates the action to be taken after encountering a certificate that has been placed on hold (suspension)	Optional. The SIP may include a holdInstructionCode only if the SIP is requesting suspension.

[8] Refer to Appendix B for valid signature algorithm values.

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
protection	signature of message	Required. Must be calculated according to MSG_SIG_ALG

3.2 FPKI SSP Revocation Response

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
sender	the name of the CA who produced the message	Required. Data type must be directoryName Value must be the SubjectDN in the FPKI SSP CA certificate.
recipient	the name of the SIP which requested the certificate	Required. Data type must be directoryName Value must be the SubjectDN in the SIP SCI Issued Certificate.
messageTime	time at which the CA produced the message	Required
protectectionAlg	signature algorithm used to protect this message	Required. MSG_SIG_ALG[9]
senderKID	the reference number which the CA has previously issued to the end entity (together with the MACing key)	Must not be used.
transactionID	value from corresponding request message	Required. Use corresponding value from SIP Authentication Certificate Request.
senderNonce	128 random bits used to protect against replay attacks	Required.
recipNonce	128 random bits used to protect against replay attacks	Required. Value from senderNonce from certificate response message.
rrc	revocation response content structure	Required.
rrc.status	processing status structure in response to the request	Required.
rrc.status.status	status code describing processing status	Required.

[9] Refer to Appendix B for valid signature algorithm values.

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
rrc.status.statusString	human readable information	Optional.
rrc.status.failInfo	additional information regarding processing a request	Optional. An FPKI SSP may return additional failure information if revocation request could not be processed.
rrc.revCerts	IDs for certificates which revocation was requested	Optional.
rrc.crls	the resulting CRLs that are produced by the FPKI SSP	Optional.
freeText	human readable information	Optional. Values may be: “<CA> successfully received certificate revocation request”
protection	signature of message	Required. Must be calculated according to MSG_SIG_ALG.
extraCerts	additional certificates	Must not be used.

4 PIV Authentication Certificate Suspension

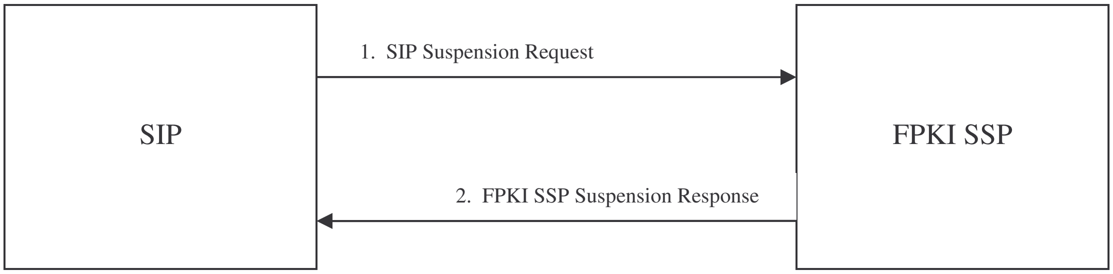
[SCI Architecture] requires a SIP to request a suspension of an FPKI SSP issued certificate on behalf of the end user. The transaction consists of two (2) messages between the SIP and FPKI SSP:

1. SIP suspension request; and
2. FPKI SSP suspension response

A SIP MUST NOT request that more than one certificate is suspended in one SIP suspension request. The PIV authentication certificate suspension transaction is essentially the same as the revocation transaction. The only difference is that the optional reason code MUST be used.

Figure 4-1 presents a high-level sequence diagram of the transactions.

Figure 4-1: Transaction Sequence Diagram



4.1 SIP Suspension Request

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
sender	the name identifying the SIP	Required. Data type must be directoryName. Value must be the SubjectDN in the SIP SCI Issued Certificate
recipient	the name of the CA who is being asked to produce a certificate	Required. Data type must be directoryName. Use the value of SubjectDN in the FPKI SSP CA certificate.
protectionAlg	signature algorithm used to protect this message	Required. MSG_SIG_ALG[10]
senderKID	the reference number which the CA has previously issued to the end entity (together with the MACing key)	Must Not be used
transactionID	unique id sent from the SIP to the FPKI SSP	Required. Combination of SIP unique identifier issued by the SCI governing Authority plus 20 random bytes.
senderNonce	128 random bits used to protect against replay attacks	Required. 128 Random Bits
freeText	human readable information	Must not be used
rrc	revocation request content structure	Required.
rrc.certDetails.serialNumber	uniquely identifies the end certificate	Required. The SIP may include other fields in the certificate template such as subject
rrc.crlEntryDetails.reasonCode	the reasonCode is a non-critical CRL entry extension that identifies the reason for the certificate revocation	Required. The SIP MUST include a reason code of certificateHold if the SIP is requesting a suspension of the certificate.

[10] Refer to Appendix B for valid signature algorithm values.

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
rrc.crlEntryDetails.holdInstructionCode	indicates the action to be taken after encountering a certificate that has been placed on hold (suspension)	Optional. The SIP may include a holdInstructionCode only if the SIP is requesting suspension.
protection	signature of message	Required. Must be calculated according to MSG_SIG_ALG

4.2 FPKI SSP Suspension Response

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
sender	the name of the CA who produced the message	Required. Data type must be directoryName Value must be the SubjectDN in the FPKI SSP CA certificate.
recipient	the name of the SIP which requested the certificate	Required. Data type must be directoryName Value must be the SubjectDN in the SIP SCI Issued Certificate.
messageTime	time at which the CA produced the message	Required
protectectionAlg	signature algorithm used to protect this message	Required. MSG_SIG_ALG[11]
senderKID	the reference number which the CA has previously issued to the end entity (together with the MACing key)	Must not be used.
transactionID	value from corresponding request message	Required. Use corresponding value from SIP Authentication Certificate Request.
senderNonce	128 random bits used to protect against replay attacks	Required.
recipNonce	128 random bits used to protect against replay attacks	Required. Value from senderNonce from certificate response message.
rrc	revocation response content structure	Required.

[11] Refer to Appendix B for valid signature algorithm values.

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
rrc.status	processing status structure in response to the request	Required.
rrc.status.status	status code describing processing status	Required.
rrc.status.statusString	human readable information	Optional.
rrc.status.failInfo	additional information regarding processing a request	Optional. An FPKI SSP may return additional failure information if revocation request could not be processed.
rrc.revCerts	IDs for certificates which revocation was requested	Optional.
rrc.crls	the resulting CRLs that are produced by the FPKI SSP	Optional.
freeText	human readable information	Optional. Values may be: "<CA> successfully received certificate suspension request"
protection	signature of message	Required. Must be calculated according to MSG_SIG_ALG.
extraCerts	additional certificates	Must not be used.

5 PIV Authentication Certificate Un-Suspension

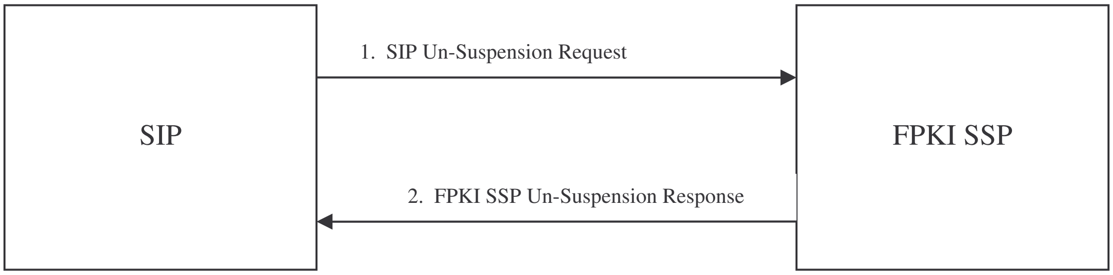
[SCI Architecture] requires a SIP to request un-suspension of an FPKI SSP issued certificate on behalf of the end user. The transaction consists of two (2) messages between the SIP and FPKI SSP:

3. SIP un-suspension request; and
4. FPKI SSP un-suspension response

A SIP MUST NOT request that more than one certificate is un-suspended in one SIP un-suspension request.

Figure 5-1 presents a high-level sequence diagram of the transactions.

Figure 5-1: Transaction Sequence Diagram


1. SIP Un-Suspension Request
SIP
FPKI SSP
2. FPKI SSP Un-Suspension Response

5.1 SIP Un-Suspension Request

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
sender	the name identifying the SIP	Required. Data type must be directoryName. Value must be the SubjectDN in the SIP SCI Issued Certificate
recipient	the name of the CA who is being asked to produce a certificate	Required. Data type must be directoryName. Use the value of SubjectDN in the FPKI SSP CA certificate.
protectionAlg	signature algorithm used to protect this message	Required. MSG_SIG_ALG[12]
senderKID	the reference number which the CA has previously issued to the end entity (together with the MACing key)	Must Not be used
transactionID	unique id sent from the SIP to the FPKI SSP	Required. Combination of SIP unique identifier issued by the SCI governing Authority plus 20 random bytes.
senderNonce	128 random bits used to protect against replay attacks	Required. 128 Random Bits
freeText	human readable information	Must not be used
rrc	revocation request content structure	Required.
rrc.certDetails.serialNumber	uniquely identifies the end certificate	Required. The SIP may include other fields in the certificate template such as subject
rrc.crlEntryDetails.reasonCode	the reasonCode is a non-critical CRL entry extension that identifies the reason for the certificate revocation	Required. The SIP MUST include a reason code of removeFromCRL if the SIP is requesting an un-suspension of the certificate.

[12] Refer to Appendix B for valid signature algorithm values.

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
protection	signature of message	Required. Must be calculated according to MSG_SIG_ALG

5.2 FPKI SSP Un-Suspension Response

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
sender	the name of the CA who produced the message	Required. Data type must be directoryName Value must be the SubjectDN in the FPKI SSP CA certificate.
recipient	the name of the SIP which requested the certificate	Required. Data type must be directoryName Value must be the SubjectDN in the SIP SCI Issued Certificate.
messageTime	time at which the CA produced the message	Required
protectectionAlg	signature algorithm used to protect this message	Required. MSG_SIG_ALG[13]
senderKID	the reference number which the CA has previously issued to the end entity (together with the MACing key)	Must not be used.
transactionID	value from corresponding request message	Required. Use corresponding value from SIP Authentication Certificate Request.
senderNonce	128 random bits used to protect against replay attacks	Required.
recipNonce	128 random bits used to protect against replay attacks	Required. Value from senderNonce from certificate response message.
rrc	revocation response content structure	Required.
rrc.status	processing status structure in response to the request	Required.
rrc.status.status	status code describing processing status	Required.

[13] Refer to Appendix B for valid signature algorithm values.

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
rrc.status.statusString	human readable information	Optional.
rrc.status.failInfo	additional information regarding processing a request	Optional. An FPKI SSP may return additional failure information if revocation request could not be processed.
rrc.revCerts	IDs for certificates which revocation was requested	Optional.
rrc.crls	the resulting CRLs that are produced by the FPKI SSP	Optional.
freeText	human readable information	Optional. Values may be: "<CA> successfully received certificate un-suspension request"
protection	signature of message	Required. Must be calculated according to MSG_SIG_ALG.
extraCerts	additional certificates	Must not be used.

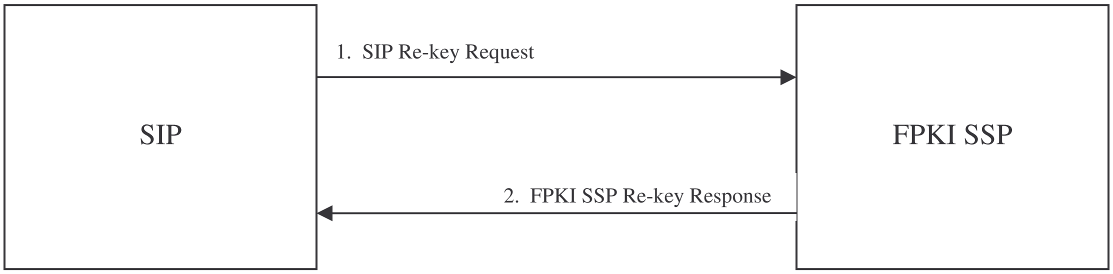
6 Certificate Re-key

[SCI Architecture] requires a SIP to request a certificate re-key of an FPKI SSP issued certificate on behalf of the end user. Certificate re-key consists of two (2) messages between the SIP and FPKI SSP:

1. Certificate re-key request
2. Certificate re-key response

Figure 6-1 presents a high-level sequence diagram of the transactions.

Figure 6-1: Transaction Sequence Diagram



The following sections describe fields and constraints of each message.

6.1 SIP Certificate Re-key Request

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
sender	the name identifying the SIP	Required. Data type must be directoryName Value must be the SubjectDN in the SIP SCI Issued Certificate
recipient	the name of the CA who is being asked to produce a certificate	Required. Data type must be directoryName. Use the value of SubjectDN in the CA certificate.
protectionAlg	signature algorithm used to protect this message	Required. MSG_SIG_ALG[14]
senderKID	the reference number which the CA has previously issued to the end entity (together with the MACing key)	Must Not be used
transactionID	unique id sent from the SIP to the FPKI SSP	Required. Combination of SIP unique identifier issued by the SCI Governing Authority plus 20 random bytes.
senderNonce	128 random bits used to protect against replay attacks	Required. 128 Random Bits
freeText	human readable information	Not used
kur.crm	certificate re-key request structure	Required.
kur.crm[0].certReq.certReqId	index of certificate update request messages	Required. Fixed value of 0
kur.crm[0].certReq.certTemplate	describes fields that the SIP wishes to contain in the certificate	Required. Only subject public key is allowed for certificate re-key.
kur.crm[0].certReq.certTemplate.publicKey	subject public key	Required. Must contain the subject public key. [15]

[14] Refer to Appendix B for valid signature algorithm values.

[15] Public key algorithm must be RSA or ECDSA. Refer to [SP800-78] for details.

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
kur.crm[0].certReq.controls.OldCertId	specifies the certificate to be updated by the current certification request	Required.
kur.crm[0].pop.POPOSigningKey	proof of possession of the private signing key	Required.
kur.crm[0].controls.archiveOptions	a request to the FPKI SSP to archive the end user's private key	Not used. SIP may not archive the private key.
kur.crm[0].certReq.controls.publicationInfo	a request to the FPKI SSP to publish the certificate in a directory server	Optional. SIP may request that the FPKI SSP publishes the certificate
protection	signature of message	Required. Must be calculated according to MSG_SIG_ALG

6.2 FPKI SSP Certificate Re-key Response

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
sender	the name of the CA who produced the message	Required. Data type must be directoryName Use the value of SubjectDN in the FPKI SSP CA certificate
recipient	the name of the SIP which requested the certificate	Required. Data type must be directoryName. Value must be the SubjectDN in the SIP SCI Trust Certificate.
messageTime	time at which the CA produced the message	Required
protectectionAlg	signature algorithm used to protect this message	Required. MSG_SIG_ALG[16]
senderKID	the reference number which the CA has previously issued to the end entity (together with the MACing key)	Must not be used
transactionID	value from corresponding request message	Required. Use corresponding value from SIP Authentication Certificate Re-key Request.
senderNonce	128 random bits used to protect against replay attacks	Required.

[16] Refer to Appendix B for valid signature algorithm values.

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
recipNonce	128 random bits used to protect against replay attacks	Required. Value from senderNonce from certificate response message.
freeText	human readable information	Optional. Values may be: "<CA> successfully received certificate request"
kup.crc	key re-key response structure	Required.
kup.crc[0].certReqId	request id that corresponds to the request in the certificate request message	Required. fixed value of zero
kup.crc[0].status.status	status message	Required. Values may be: "accepted" "rejection"
kup.crc[0].status.failInfo	message explaining why certificate generation failed	Optional. Use only if crc[0].status.status = "rejection"
kup.crc[0].certifiedKeyPair	structure that contains the certificate	Required if certificate request was accepted
kup.crc[0].certifiedKeyPair.certificate	certificate	Required
kup.crc[0].certifiedKeyPair.encryptedCert	encryption certificate	Must not be used
kup.crc[0].certifiedKeyPair.publicationInfo	indicates where the certificate has been published	Optional. Present only if SIP requests that the certificate is published
protection	signature of message	Required. Must be calculated according to MSG_SIG_ALG.
extraCerts	additional certificates	Optional. The FPKI SSP may provide extra certificates that would facilitate path validation.

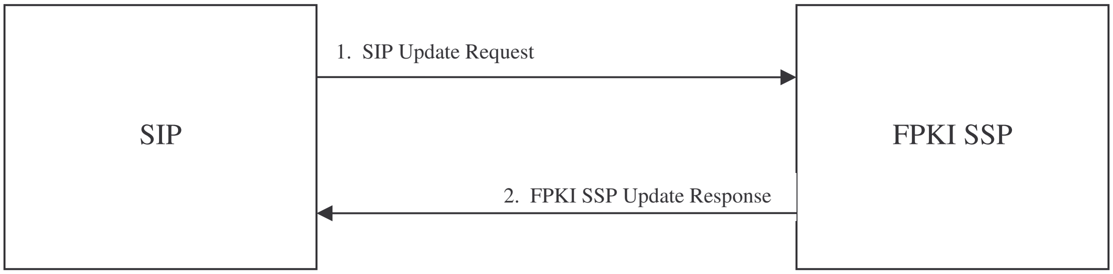
7 Certificate Update

[SCI Architecture] requires a SIP to request a certificate update of an FPKI SSP issued certificate on behalf of the end user. Certificate update consists of two (2) messages between the SIP and FPKI SSP:

3. Certificate update request
4. Certificate update response

Figure 6-1 presents a high-level sequence diagram of the transactions.

Figure 7-1: Transaction Sequence Diagram



The following sections describe fields and constraints of each message.

7.1 SIP Certificate Update Request

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
sender	the name identifying the SIP	Required. Data type must be directoryName Value must be the SubjectDN in the SIP SCI Issued Certificate
recipient	the name of the CA who is being asked to produce a certificate	Required. Data type must be directoryName. Use the value of SubjectDN in the CA certificate.
protectionAlg	signature algorithm used to protect this message	Required. MSG_SIG_ALG[17]
senderKID	the reference number which the CA has previously issued to the end entity (together with the MACing key)	Must Not be used
transactionID	unique id sent from the SIP to the FPKI SSP	Required. Combination of SIP unique identifier issued by the SCI Governing Authority plus 20 random bytes.
senderNonce	128 random bits used to protect against replay attacks	Required. 128 Random Bits
freeText	human readable information	Not used
kur.crm	certificate request structure	Required.
kur.crm[0].certReq.certReqId	index of certificate update request messages	Required. Fixed value of 0
kur.crm[0].certReq.certTemplate	describes fields that the SIP wishes to contain in the certificate	Required. SIP may include updatable items such as public key, name, etc.
kur.crm[0].certReq.controls.OldCertId	specifies the certificate to be updated by the current certification request	Required.
kur.crm[0].pop.POPOSigningKey	proof of possession of the private signing key	Optional. Only use when subject is updating his/her public key.

[17] Refer to Appendix B for valid signature algorithm values.

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
kur.crm[0].controls.archiveOptions	a request to the FPKI SSP to archive the end user's private key	Not used. SIP may not archive the private key.
kur.crm[0].certReq.controls.publicationInfo	a request to the FPKI SSP to publish the certificate in a directory server	Optional. SIP may request that the FPKI SSP publishes the certificate
protection	signature of message	Required. Must be calculated according to MSG_SIG_ALG

7.2 FPKI SSP Certificate Update Response

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
sender	the name of the CA who produced the message	Required. Data type must be directoryName Use the value of SubjectDN in the FPKI SSP CA certificate
recipient	the name of the SIP which requested the certificate	Required. Data type must be directoryName. Value must be the SubjectDN in the SIP SCI Trust Certificate.
messageTime	time at which the CA produced the message	Required
protectectionAlg	signature algorithm used to protect this message	Required. MSG_SIG_ALG[18]
senderKID	the reference number which the CA has previously issued to the end entity (together with the MACing key)	Must not be used
transactionID	value from corresponding request message	Required. Use corresponding value from SIP Authentication Certificate Request.
senderNonce	128 random bits used to protect against replay attacks	Required.
recipNonce	128 random bits used to protect against replay attacks	Required. Value from senderNonce from certificate response message.

[18] Refer to Appendix B for valid signature algorithm values.

[RFC 4210] FIELD	DESCRIPTION	SCI CONSTRAINTS
freeText	human readable information	Optional. Values may be: "<CA> successfully received certificate request"
kup.crc	key update response structure	Required.
kup.crc[0].certReqId	request id that corresponds to the request in the certificate request message	Required. fixed value of zero
kup.crc[0].status.status	status message	Required. Values may be: "accepted" "rejection"
kup.crc[0].status.failInfo	message explaining why certificate generation failed	Optional. Use only if crc[0].status.status = "rejection"
kup.crc[0].certifiedKeyPair	structure that contains the certificate	Required if certificate update request was accepted
kup.crc[0].certifiedKeyPair.certificate	certificate	Required
kup.crc[0].certifiedKeyPair.encryptedCert	encryption certificate	Must not be used
kup.crc[0].certifiedKeyPair.publicationInfo	indicates where the certificate has been published	Optional. Present only if SIP requests that the certificate is published
protection	signature of message	Required. Must be calculated according to MSG_SIG_ALG.
extraCerts	additional certificates	Optional. The FPKI SSP may provide extra certificates that would facilitate path validation.

Appendix A: Glossary & Acronyms

Term	Description
Certificate	Per [Common Policy], a digital representation of information which at least (1) identifies the CA issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the CA issuing it. [ABADSG]. As used in this CP, the term "Certificate" refers to certificates that expressly reference the OID of this CP in the "Certificate Policies" field of an X.509 v.3 certificate.
HyperText Transfer Protocol, Secure (HTTPS)	The protocol for accessing a secure Web server. Using HTTPS in the URL instead of HTTP directs the message to a secure port number rather than the default Web port number of 80. The session is then managed by a security protocol such as Secure Socket Layer (SSL).
National Agency Check with Written Inquiries (NACI)	The basic and minimum investigation required on all new Federal employees consisting of a NAC with written inquiries and searches of records covering specific areas of an individual's background during the past five years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities). Coverage includes: – Employment, 5 years – Education, 5 years and highest degree verified – Residence, 3 years – References – Law Enforcement, 5 years – NACs
Re-key	Per [Common Policy], re-keying a certificate means that a new certificate is created that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number, and it may be assigned a different validity period.
Revocation	Per [Common Policy], to prematurely end the operational period of a certificate effective at a specific date and time. Revocation indicates that the binding between the subject and the subject's public key defined within a certificate is no longer considered valid. Upon revocation, the certificate is placed on the Certificate Revocation List (CRL) and shall be included on all new publications of the certificate status information until the certificate expires.
Suspension	Temporary revocation of a certificate.
Update	Per [Common Policy], updating a certificate means creating a new certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old certificate. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or updated.
Un-Suspension	Undo a certificate's revocation in order to reinstate the validity of the binding between the subject and the subject's public key defined within the certificate.

Acronym	Abbreviation For
ACK	Acknowledgement
ASN.1	Abstract Syntax Notation One
CA	Certification Authority
DN	Domain Name
FASC-N	Federal Agency Smart Credential Number
FIPS	Federal Information Processing Standards
FPKI	Federal Public Key Infrastructure
HSPD-12	Homeland Security Presidential Directive-12
HTTPS	Hypertext Transfer Protocol Secure
ID	Identifier
MAC	Message Acknowledgement
NACI	National Agency Check with Written Inquiries
NIST	National Institutes of Science and Technology
OMB	Office of Management and Budget
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
SIP	System Infrastructure Provider
SP	Special Publication
SSP	Shared Service Provider

Appendix B: SIP to FPKI SSP Signature Algorithm Values

Signature Algorithm	Object Identifier
RSA with SHA-1 and PKCS v1.5 padding	sha1WithRSAEncryption ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
RSA with SHA-256 and PKCS v1.5 padding	id-RSASSA-PSS ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10}
ECDSA with SHA-1	ecdsa-with-SHA1 ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) 1}
ECDSA with SHA-224	ecdsa-with-SHA224 ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 1}
ECDSA with SHA-256	ecdsa-with-SH256 ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2}