Federal Bridge Certification Authority
Product Interoperability Guidelines

September 28, 2001

The Federal Bridge Certification Authority (FBCA) is the unifying element to link autonomous Agency Certification Authorities (CAs) into a systematic overall Federal PKI. The FBCA functions as a non-hierarchical hub allowing relying party agencies to create certificate trust paths from their domains back to the domain of the agency that issued the certificate, so that the levels of assurance honored by disparate PKIs can be reconciled.

The General Services Administration (GSA), under the auspices of the Federal Public Key Infrastructure Policy Authority and the Federal PKI Steering Committee operates the FBCA. In order to promote interoperability and the appropriate use of certificate policies, the FBCA has issued a minimum set of operational requirements that support trust path creation and verification of digital signatures. The FBCA will issue cross-certificates to other agency Principal CAs, and then only as authorized by the Federal PKI Policy Authority (FPKIPA). Initially, agency CAs that operate in trust domains that meet the requirements established by the FPKIPA will be eligible to cross-certify with the FBCA.

Products used within the FBCA must be able to support the following basic requirements:

- Use or support use of a FIPS 140-1 level 3 or better CA private key generation/protection hardware device. The device must be U.S. manufactured or FPKIPA approved.
- Ability to exchange PKCS7/10 certificate request/response messaging formats: generate PKCS7/10 certificate requests and responses and export them to other CAs as files; and import and process PKCS7/10 certificate requests and responses received as files from other CAs.
- Satisfy all technical and design assurance requirements specified in the FBCA CP available on-line (from http://www.cio.gov/fbca/library/index.htm).
- Ability to export self-signed certificates to a file as a DER-encoded object or in an LDIF file.
- Support off-line export of the following in such manner that they can be imported [posted] to the Peerlogic i500 [X.500 LDAP v2 or better] directory:
  - Self-signed certificates
  - All cross certificate pairs generated
  - An Authority Revocation List (ARL) or Certificate Revocation Lists (CRLs) covering certificates revoked
- Assert, in the certificatePolicies extension field, up to all four FBCA Certificate Policy OIDs within a single X.509 cross-certificate
- Map agency-specific levels of assurance to the levels of assurance present in the certificatePolicies extension field; that mapping will be expressed in the policyMappings extension of the FBCA cross-certificates.

- Generate, issue, and maintain an Authority Revocation List (ARL) and/or Certificate Revocation Lists (CRLs).
- Generate, issue, and maintain X.509 version 3 or higher certificates and CRLs that conform to the following profile

Certificate profile:

Field	Criticality Flag	Field contents	Comments
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber			
CertificateSerialNumber		INTEGER	Positive integer, unique for the set of certificates issued by this CA
signature			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field.
algorithm		1.2.840.113549.1.1.5	SHA-1WithRSAEncryption
parameters		NULL	Always NULL for rsa with SHA-1
issuer			
Name			C=US, O=U.S. Government, OU=FBCA, OU=<product name>
RDNSequence			C= ; O= ; and OU= are required
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	use printableString (first choice), or bmpString (second choice) [Note: utf8string must be used in all certificates after December 31st, 2003.]
validity			
notBefore			
Time			
utcTime			
UTCTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime			[This encoding should not required until 2050.]
GeneralizedTime		YYYYMMDDHHMMSSZ	Use for dates after 2049

Field	Criticality Flag	Field contents	Comments
notAfter			
Time			
utcTime			
UTCTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime			[This encoding should not required until about 2044.]
GeneralizedTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
subject			
Name			X.500 Distinguished name of the owner of the certificate.
RDNSequence			C= ; O= ; OU= ; CN= ; and DC= are required.
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	The string types used to encode the subject name must match the issuer name encoding in certificates issued by this subject.
subjectPublicKeyInfo			
algorithm			
AlgorithmIdentifier			Public key algorithm used.
The next two entries apply only to RSA Public keys			
algorithm		1.2.840.113549.1.1.1	RSA Encryption
parameters		NULL	Always assert NULL in the parameters for RSA public keys
The next two entries apply only to DSA Public Keys			
algorithm		1.2.840.10040.4.1	DSA
parameters		dss-parms	Always include the parameters for DSA public keys; syntax is defined in RFC 2459.
The next entry applies to both DSA and RSA Public Keys			
subjectPublicKey		BIT STRING	
extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE		

Field	Criticality Flag	Field contents	Comments
keyIdentifier		OCTET STRING	Must match the authorityKeyIdentifier in certificates issued by the subject whose signature can be validated using the subjectPublicKey. Use the key identifier provided by the subject.
keyUsage	TRUE		
digitalSignature		1	This value MAY be asserted.
nonRepudiation		1	This value MAY be asserted.
keyEncipherment		0	This value MUST NOT be asserted.
dataEncipherment		0	This value MUST NOT be asserted.
keyAgreement		0	This value MUST NOT be asserted.
keyCertSign		1	REQUIRED. This value MUST be asserted.
cRLSign		1	This value MAY be asserted.
encipherOnly		0	This value MUST NOT be asserted.
decipherOnly		0	This value MUST NOT be asserted.
certificatePolicies	FALSE		MUST be able to assert a sequence of between one and four policies, inclusive.
PolicyInformation			
policyIdentifier			
CertPolicyId		OID	May be any of the following: {2.16.840.1.101.3.2.1.3.1, 2.16.840.1.101.3.2.1.3.2, 2.16.840.1.101.3.2.1.3.3, 2.16.840.1.101.3.2.1.3.4}
policyQualifiers			Policy qualifiers MUST NOT appear.
policyMappings	FALSE		This extension will appear in all certificates issued to Agency PCAs. This extension does not appear in certificates issued to other FBCA nodes. This extension will be non-critical in all certificates issued by the FBCA; this extension may be critical in certificates issued to the FBCA to ensure policy mapping is processed by its relying parties.
issuerDomainPolicy			
CertPolicyId		OID	OID of policy from the FBCA domain that maps to the equivalent policy in the subject CA's domain. May be any of the following: {2.16.840.1.101.3.2.1.3.1, 2.16.840.1.101.3.2.1.3.2, 2.16.840.1.101.3.2.1.3.3, 2.16.840.1.101.3.2.1.3.4}
subjectDomainPolicy			
CertPolicyId		OID	OID of policy in the subject CA's domain that maps to the equivalent policy in the issuing CA's domain.
basicConstraints	TRUE		
cA		TRUE	Default is False.
pathLenConstraint		INTEGER	This field is omitted where path length constraints are not imposed by the FBCA.

Field	Criticality Flag	Field contents	Comments
nameConstraints	TRUE		MUST appear in every certificate issued by the FBCA to a PCA. MUST NOT appear in certificates issued to other FBCA nodes.
permittedSubtrees			MUST appear in every certificate issued by the FBCA to a PCA. This field will identify legal agency name spaces.
GeneralSubtree			Support for DN name form is required. Support for DNS names and rfc 822 names is recommended.
base			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	Must match string types used to encode names in certificates issued by the subject of this certificate.
uniformResourceIdentifier		IA5String	
minimum			
BaseDistance		0	Default value of zero.
maximum			Always omitted.
BaseDistance		INTEGER	Always omitted.
excludedSubtrees			Only used if a portion of the agency PKI name space is explicitly rejected by the FBCA.
GeneralSubtrees			
GeneralSubtree			
base			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			

Field	Criticality Flag	Field contents	Comments
AttributeType		OID	
AttributeValue		See comment.	utf8string must be used in all certificates after December 31st, 2003. Prior to that, if possible, use printableString (first choice), or bmpString (second choice)
uniformResourceIdentifier		IA5String	
minimum			
BaseDistance		0	Default value of zero.
maximum			Always omitted.
BaseDistance		INTEGER	Always omitted.
policyConstraints	TRUE		This extension only appears if the FBCA wishes to inhibit policy mapping.
requireExplicitPolicy			Always omitted.
SkipCerts		0	
inhibitPolicyMapping			This may be used in the future
SkipCerts		INTEGER	
cRLDistributionPoints	FALSE		
DistributionPoint			
distributionPoint			
DistributionPointName			
fullName			
GeneralNames			
GeneralName			
directoryName			Identifies the X.500 entry that will contain the CRL which contains status information for this certificate.
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	printableString (first choice), or bmpString (second choice).
uniformResourceIdentifier		IA5String	

Field	Criticality Flag	Field contents	Comments
nameRelativeToCRLIssuer			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	utf8string must be used in all certificates after December 31st, 2003. Prior to that, if possible, use printableString (first choice), or bmpString (second choice)
reasons			
ReasonFlags			Always omitted – FBCA CRLs cover all reason codes.
cRLIssuer			Always omitted – FBCA does not issue indirect CRLs.

CRL profile:

Field	Criticality Flag	Field contents	Comments
CertificateList			
tbsCertList			Fields to be signed.
version		1	Integer Value of "1" for Version 2 CRL.
signature			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field.
algorithm			
		1.2.840.113549.1.1.5	SHA-1WithRSAEncryption
parameters		NULL	Always NULL for SHA-1withRSA
issuer			
Name			
RDNSequence			C= ; O= ; and OU= are required
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		See comment.	String types used to encode name MUST match subject field in certificate used to validate the signature on this CRL.

Field	Criticality Flag	Field contents	Comments
thisUpdate			
Time			
utcTime			
UTCTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime			
GeneralizedTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
nextUpdate			
Time			MUST appear in all CRLs.
utcTime			
UTCTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime			
GeneralizedTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
revokedCertificates			
userCertificate			
CertificateSerialNumber		INTEGER	Integer of certificate being revoked
revocationDate			
Time			
utcTime			
UTCTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime			
GeneralizedTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
crlEntryExtensions			
reasonCode	FALSE		If no reason is specified, this extension is omitted. As the fBCA does not issue delta CRLs, the reason cannot be removeFromCRL.
CRLReason			Any CRLReason may be asserted, except *unspecified* and *removeFromCRL*
invalidityDate	FALSE		If the certificate is believed to have been compromised before the date of revocation, this extension should be included.
GeneralizedTime		YYYYMMDDHHMMSSZ	Contains the date on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid.
crlExtensions			
cRLNumber	FALSE	INTEGER	MUST appear in all CRLs. Monotonically increasing sequential number.

Field	Criticality Flag	Field contents	Comments
authorityKeyIdentifier	FALSE		MUST appear in all CRLs.
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key. (Matches the subjectKeyIdentifier in certificates that can be used to validate this CRL..)