FPKIPA
Federal Public Key Infastructure Policy Authority

Shared Service Provider
Repository Service Requirements

Federal PKI Policy Authority
Shared Service Provider Working Group

June 28, 2007

Introduction

This document outlines the requirements vendors must meet in their repository service offering in order to become certified under the PKI Shared Service Provider (SSP) Program. Tables I, II, and III contain lists of mandatory requirements that must be met by all vendors as a certified PKI SSP. Table IV contains the list of requirements that must be met by vendors that include end user certificates in their repositories. Requirements that are specified as applying to a provider's Certification Authority (CA) apply to all CAs operated by that provider. All requirements were derived from at least one of the following documents: [X.509], [RFC 2585], [RFC 2616], [RFC 2798], [RFC 3851], [RFC 4511], [RFC 4519], [RFC 4523], [COMMON], and [GDS].

	Table I - Mandatory Repository Service Requirements	Reference
1	The repository service shall contain all CA certificates issued to or by the provider's CA, including self-issued certificates. Self-signed certificates do not need to be included in the repository.	[COMMON]
2	The repository service shall contain all Certificate Revocation Lists (CRLs) issued by the provider's CA.	[COMMON]
3	The repository service shall allow unauthenticated access by the public to the information (CA certificates and CRLs) within the directory.	[COMMON]
4	The repository service shall be designed and implemented so as to provide 99% availability overall and limit scheduled down-time to 0.5% annually.	[COMMON]
5	The repository service shall provide an average three second response time (or less) from the time the repository receives the request until it delivers the response to the network.	[GDS]
6	For each certificate issued by the provider's CA, for each distribution point in the certificate's cRLDistributionPoints extension, the corresponding CRL shall be available from the location indicated in the distribution point name.	[X.509]

	Table II - Mandatory Repository Service Lightweight Directory Access Protocol (LDAP) Access Requirements	Reference
1	The repository service shall provide at minimum a Lightweight Directory Access Protocol (LDAP) interface at the port 389, supporting both LDAP versions 2 and 3.	[COMMON] [RFC 4511]

	Table II - Mandatory Repository Service Lightweight Directory Access Protocol (LDAP) Access Requirements	Reference
2	The distinguished names (DNs) of directory entries may be in either of two forms: a geo-political name or an Internet domain component name. Geo-political distinguished names shall be composed of any combination of the following attributes: country (c); organization (o); organizational unit (ou); and common name (cn). Internet domain component names shall be composed any combination of the following attributes: domain component (dc); organizational unit (ou); and common name (cn).	[COMMON]
3	The CA's entry shall use at least one of the following as a base object class: person, organizationalPerson, inetOrgPerson, or organizationalUnit.	[RFC 2798] [RFC 4519]
4	The CA's entry shall include the auxiliary object class pkiCA.	[RFC 4523]
5	The CA's entry shall include the commonName or organizationalUnitName attribute.	[RFC 4519]
6	The cACertificate attribute of a CA's directory entry shall hold all certificates issued to the CA, including self-issued certificates.	[X.509] [RFC 4523]
7	The issuedToThisCA (forward) elements of the crossCertificatePair attribute of a CA's directory entry shall hold all certificates, except self-issued certificates, issued to the CA.	[X.509] [RFC 4523]
8	The issuedByThisCA (reverse) elements of the crossCertificatePair attribute of a CA's directory entry shall hold all certificates issued by the CA to other CAs.	[X.509] [RFC 4523]
9	When both the issuedToThisCA (forward) and issuedByThisCA (reverse) elements of the crossCertificatePair attribute are present in a single attribute value of a CA's directory entry, the issuer name in one certificate shall match the subject name in the other and vice versa.	[X.509] [RFC 4523]
10	When both the issuedToThisCA (forward) and issuedByThisCA (reverse) elements of the crossCertificatePair attribute are present in a single attribute value of a CA's directory entry, the subject public key in one certificate shall be capable of verifying the digital signature on the other certificate and vice versa.	[X.509] [RFC 4523]
11	Each CRL issued by the provider's CA shall be stored in the all of the directory entries specified in a distribution point name in the issuingDistributionPoint extension of the CRL.	[X.509] [RFC 4523]

	Table II - Mandatory Repository Service Lightweight Directory Access Protocol (LDAP) Access Requirements	Reference
12	Each CRL issued by the provider's CA that does not include an issuingDistributionPoint extension or includes an issuingDistributionPoint extension that does not include the distributionPoint field shall be stored in the CA's directory entry.	[X.509] [RFC 4523]
13	Each CRL issued by the provider's CA that includes an issuingDistributionPoint extension with onlyContainsCACerts set to TRUE shall be stored in the authorityRevocationList attribute of the appropriate directory entry or entries.	[X.509] [RFC 4523]
14	Each CRL issued by the provider's CA that does not include an issuingDistributionPoint extension or includes an issuingDistributionPoint extension with onlyContainsCACerts set to FALSE shall be stored in the certificateRevocationList attribute of the appropriate directory entry or entries.	[X.509] [RFC 4523]

	Table III - Mandatory Repository Service Hyper Text Transmission Protocol (HTTP) Access Requirements	Reference
1	The repository service shall provide at minimum a Hyper Text Transmission Protocol (HTTP) version 1.1 interface at the port 80.	[RFC 2616]
2	CRLs issued by the provider's CA shall be stored in files with a .crl extension. Each file shall contain a single DER-encoded CRL.	[RFC 2585]
3	CA certificates issued to the provider's CA shall be stored as a degenerate signedData "certs-only" message in a file with a .p7c extension. (This includes self-issued certificates.)	[RFC 3851]
4	CA certificates issued by the provider's CA shall be stored as a degenerate signedData "certs-only" message in a file with a .p7c extension. (This includes self-issued certificates.)	[RFC 3851]

	Table IV – End Entity Certificate Repository Service Requirements	Reference
1	End entity entries shall use one of the following classes: person or device.	[RFC 4519]
2	End entity entries shall use the pkiUser class.	[RFC 4523]
3	End entity certificates that are placed in the directory shall be placed in the userCertificate attribute of the certificate subject's directory entry.	[RFC 4523]

	Table IV – End Entity Certificate Repository Service Requirements	Reference
4	Certificates that contain the FASC-N in the subject alternative name extension, such as PIV Authentication certificates and Card Authentication certificates, shall not be distributed via public repositories (e.g., via LDAP or HTTP).	[COMMON]

References

[X.509] ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

[RFC 2585] Russell Housley, and Paul Hoffman, "Internet X.509 Public Key Infrastructure: Operational Protocols: FTP and HTTP", RFC 2585, May 1999.

[RFC 2616] Roy T. Fielding, James Gettys, Jeffrey C. Mogul, Henrik Frystyk Nielsen, Larry Masinter, Paul J. Leach, and Tim Berners-Lee, "Hypertext Transfer Protocol – HTTP/1.1", June 1999.

[RFC 2798] Mark Smith, "Definition of the inetOrgPerson LDAP Object Class", RFC 2798, April 2000.

[RFC 3851] Blake Ramsdell, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification", RFC 3851, July 2004.

[RFC 4511] Jim Sermersheim, "Lightweight Directory Access Protocol (LDAP): The Protocol", RFC 4511, June 2006.

[RFC 4519] Andrew Sciberras, "Lightweight Directory Access Protocol (LDAP): Schema for User Applications", RFC 4519, June 2006.

[RFC 4523] Kurt D. Zeilenga, "Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates", RFC 4523, June 2006.

[COMMON] X.509 Certificate Policy for the Common Policy Framework, Version 3647 – 1.0, May 8, 2007.

[GDS] "GLOBAL DIRECTORY SERVICE: Requirements Identification Document", Version 1.0, September 4, 2001.