Common Policy CA Change Proposal Number: 2011-03

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Proposed modifications to the Federal Common Policy Framework Certificate Policy
Date: September 20, 2011

Title: Remove requirements for Lightweight Directory Access Protocol (LDAP) references in certificates

Version and Date of Certificate Policy Requested to be changed: 1) *X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework*; and 2) *X.509 Certificate and CRL Extensions Profile for the Shared Service Providers (SSP) Program*

Change Advocate's Contact Information:

Name: *Cheryl Jenkins*
Organization: *Federal PKI Management Authority (FPKIMA)*
Telephone number: *202-577-1441*
E-mail address: *cheryl.jenkins@gsa.gov*

Organization requesting change: *FPKIMA*

Change summary: This change eliminates the mandatory requirements to include LDAP references in certificates. It also changes the repository requirement from specifically identifying LDAP, to a more general requirement of supporting all Uniform Resource Identifiers (URIs) in valid certificates issued by the associated CA.

Background: This is the initial step in the FPKIMA's phased approach for eliminating the requirement to provide and support LDAP accessibility. The FPKIMA has been considering a Hypertext Transfer Protocol (HTTP)-only repository model for many years. HTTP is a more cost effective and more robust repository than LDAP. HTTP is widely adopted and provides more options for high availability than LDAP, and therefore provides more security against denial of service attacks. Additionally, LDAP is often blocked at firewalls, causing delays and failed validation attempts for FPKI Relying Parties (RPs) pursuing LDAP URI references.

This change will allow the FPKIMA (and Affiliates) to stop asserting LDAP URI references in certificates. However, existing certificates and newly-issued certificates with LDAP URI references will remain acceptable. All Certification Authorities (CAs) are still required to publish certificates in a repository that is accessible through the URIs

asserted in valid certificates (i.e., a CA's repository must support every URI that the CA has asserted in valid certificates, including LDAP), but will have no obligation to support any particular protocol if there are no corresponding references in valid certificates.

Section 2.1 of *X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework* will be updated to remove the requirement for LDAP (and HTTP) support. The new text will require support for all URIs asserted in a valid certificate, and the new text will not name any specific protocols. In addition, sections 2.1, 2.2.1, 5.1.3, 6.1.4, and 6.7 of the Federal Common Policy Framework Certificate Policy will also be updated to change "directory" references to "repository" references.

X.509 Certificate and CRL Extensions Profile for the SSP Program will be updated to remove all requirements to assert LDAP URIs in certificates. This change ensures that LDAP is always "optional" in the CRL Distribution Point (CDP), Subject Information Access (SIA), and Authority Information Access (AIA) extensions. The change will also ensure that HTTP is always mandatory in the CDP, SIA, and AIA extensions.

The following X.509 Certificate and CRL Extensions Profile for the SSP Program worksheets will be updated:

- Worksheet #1: Self-Signed Certificate Profile
- Worksheet #2: Self-Issued CA Certificate Profile
- Worksheet #3: Cross Certificate Profile
- Worksheet #5: End Entity Signature Certificate Profile
- Worksheet #6: Key Management Certificate Profile
- Worksheet #7: Certificate Profile for Computing and Communications Devices
- Worksheet #8: Card Authentication Certificate Profile
- Worksheet #9: PIV Authentication Certificate Profile

Specific Changes:

Insertions are underlined, deletions are in ~~strikethrough~~:

X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework

2.1 REPOSITORIES

All CAs that issue certificates under this policy are obligated to post all CA certificates issued by or to the CA and CRLs issued by the CA in a ~~directory~~ repository that is publicly accessible through all Uniform Resource Identifier (URI) references asserted in valid certificates issued by that CA ~~the Lightweight Directory Access Protocol (LDAP) and Hypertext Transport Protocol (HTTP)~~. Specific requirements are found in *Shared Service Provider Repository Service Requirements* 9 [SSP REP]. CAs may optionally post subscriber certificates in this ~~directory~~ repository in accordance with agency policy, except as noted in section 9.4.3. To promote consistent access to certificates and CRLs, the repository shall implement access controls and communication mechanisms to prevent unauthorized modification or deletion of information.

Posted certificates and CRLs may be replicated in additional repositories for performance enhancement. Such repositories may be operated by the CA or other parties (e.g., Federal agencies).

2.2.1 Publication of Certificates and Certificate Status

The publicly accessible ~~directory~~ repository system shall be designed and implemented so as to provide 99% availability overall and limit scheduled down-time to 0.5% annually. Where applicable, the certificate status server (CSS) shall be designed and implemented so as to provide 99% availability overall and limit scheduled down-time to 0.5% annually.

5.1.3 Power and Air Conditioning

The CA shall have backup capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown. The ~~directories~~ repositories (containing CA certificates and CRLs) shall be provided with uninterrupted power sufficient for a minimum of 6 hours operation in the absence of commercial power, to maintain availability and avoid denial of service.

6.1.4 CA Public Key Delivery to Relying Parties

Practice Note: To ensure the availability of the new public key, the key rollover certificates must be distributed using ~~directories and other~~ repositories.

6.7 NETWORK SECURITY CONTROLS

A network guard, firewall, or filtering router must protect network access to CA equipment. The network guard, firewall, or filtering router shall limit services allowed to and from the CA equipment to those required to perform CA functions.

Protection of CA equipment shall be provided against known network attacks. All unused network ports and services shall be turned off. Any network software present on the CA equipment shall be necessary to the functioning of the CA application.

Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment.

~~Directories~~ Repositories, certificate status servers, and remote workstations used to administer the CAs shall employ appropriate network security controls. Networking equipment shall turn off unused network ports and services. Any network software present shall be necessary to the functioning of the equipment.

The CA shall establish connection with a remote workstation used to administer the CA only after successful authentication of the remote workstation at a level of assurance commensurate with that of the CA.

X.509 Certificate and CRL Extensions Profile for the SSP Program

Worksheet 1: Self-Signed Certificate Profile

subjectInfoAccess			
accessMethod		id-ad-caRepository (1.3.6.1.5.5.7.48.5)	Each self-signed certificate must include at least ~~two~~ one instance~~s~~ of this access method~~: one that includes the URI name form to specify the location of an LDAP-accessible directory server and one~~ that ~~includes~~ uses a URI name form to specify an HTTP accessible ~~Web~~ server. Each URI must point to a location where certificates issued by the subject of this certificate may be found.

Worksheet 2: Self-Issued CA Certificate Profile

cRLDistributionPoints	FALSE		This extension is required in all CA certificates and must contain at least ~~two URIs: one LDAP and~~ one HTTP URI. The reasons and cRLIssuer fields must be omitted.
authorityInfoAccess			authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information

			about this certificate. Certificates issued under the Common Certificate Policy must include an authorityInfoAccess extension with at least ~~two~~ one instance~~s~~ of the caIssuers access method~~:~~ ~~one that specifies an LDAP URI and one~~ that specifies an HTTP URI. The OCSP access method may also be included if status information for this certificate is available via OCSP.
subjectInfoAccess			
accessMethod		id-ad-caRepository (1.3.6.1.5.5.7.48.5)	Each CA certificate must include at least ~~two~~ one instance~~s~~ of this access method~~: one that includes the URI name form to specify the location of an LDAP accessible directory server and one~~ that ~~includes~~ uses a URI name form to specify an HTTP accessible ~~Web~~ server. Each URI must point to a location where certificates issued by the subject of this certificate may be found.

Worksheet 3: Cross Certificate Profile

cRLDistributionPoints	FALSE		This extension is required in all CA certificates and must contain at least ~~two URIs: one LDAP and~~ one HTTP URI. The reasons and cRLIssuer fields must be omitted.
authorityInfoAccess			authorityInfoAccess consists

			of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued under the Common Certificate Policy must include an authorityInfoAccess extension with at least ~~two~~ one instance~~s~~ of the caIssuers access method~~:~~ ~~one that specifies an LDAP URI and one~~ that specifies an HTTP URI. The OCSP access method may also be included if status information for this certificate is available via OCSP.
subjectInfoAccess			
accessMethod		id-ad-caRepository (1.3.6.1.5.5.7.48.5)	Each CA certificate must include at least ~~two~~ one instance~~s~~ of this access method~~: one that includes the URI name form to specify the location of an LDAP accessible directory server and one~~ that ~~includes~~ uses a URI name form to specify an HTTP accessible ~~Web~~ server. Each URI must point to a location where certificates issued by the subject of this certificate may be found.

Worksheet 5: End Entity Signature Certificate Profile

cRLDistributionPoints	FALSE		This extension is required in all end entity certificates and must contain at least ~~two URIs: one LDAP and~~ one HTTP URI. The reasons and cRLIssuer fields must be omitted.
authorityInfoAccess			authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued under the Common Certificate Policy must include an authorityInfoAccess extension with at least ~~two~~ one instance~~s~~ of the caIssuers access method~~:~~ ~~one that specifies an LDAP URI and one~~ that specifies an HTTP URI. The OCSP access method may also be included if status information for this certificate is available via OCSP.

Worksheet 6: Key Management Certificate Profile

cRLDistributionPoints	FALSE		This extension is required in all end entity certificates and must contain at least ~~two URIs: one LDAP and~~ one HTTP URI. The reasons and cRLIssuer fields must be omitted.

authorityInfoAccess			authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued under the Common Certificate Policy must include an authorityInfoAccess extension with at least ~~two~~ one instances~~:~~ of the caIssuers access method~~:~~ ~~one that specifies an LDAP URI and one~~ that specifies an HTTP URI. The OCSP access method may also be included if status information for this certificate is available via OCSP.

Worksheet 7: Certificate Profile for Computing and Communications Devices

cRLDistributionPoints	FALSE		This extension is required in all end entity certificates and must contain at least ~~two URIs: one LDAP and~~ one HTTP URI. The reasons and cRLIssuer fields must be omitted.
authorityInfoAccess			authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating

			an OCSP server that provides status information about this certificate. Certificates issued under the Common Certificate Policy must include an authorityInfoAccess extension with at least ~~two~~ one instance~~s~~ of the caIssuers access method~~:~~ ~~one that specifies an LDAP URI and one~~ that specifies an HTTP URI. The OCSP access method may also be included if status information for this certificate is available via OCSP.

Worksheet 8: Card Authentication Certificate Profile

cRLDistributionPoints	FALSE		This extension is required in all end entity certificates and must contain at least ~~two URIs: one LDAP and~~ one HTTP URI. The reasons and cRLIssuer fields must be omitted.
authorityInfoAccess			authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued under the Common Certificate Policy must include an authorityInfoAccess extension with at least ~~two~~

			one instances of the caIssuers access method: one that specifies an LDAP URI and one that specifies an HTTP URI. The OCSP access method may also be included if status information for this certificate is available via OCSP.

Worksheet 9: PIV Authentication Certificate Profile

cRLDistributionPoints	FALSE		This extension is required in all end entity certificates and must contain at least two URIs: one LDAP and one HTTP[2] URI. The reasons and cRLIssuer fields must be omitted.
authorityInfoAccess			authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued under the Common Certificate Policy must include an authorityInfoAccess extension with at least two one instances of the caIssuers access method: one that specifies an LDAP URI and one that specifies an HTTP URI. The OCSP access method must also be included since FIPS 201 mandates OCSP distribution of status information for this

			certificate.

Estimated Cost:

There is no cost to implement this change.

Implementation Date:

This change will be effective upon approval by the FPKIPA and incorporation into the Federal Common Policy Framework Certificate Policy.

Prerequisites for Adoption:

There are no prerequisites for adoption of the provision to make the use of HTTP, vice LDAP, mandatory. Elimination of support for LDAP by the FPKIMA must be approved by the FPKIPA following a determination that FBCA cross certified entities no longer require LDAP support.

Plan to Meet Prerequisites:

The FPKIMA will develop a plan for the eventual elimination of LDAP support for submission to the FPKIPA for approval.

Approval and Coordination Dates:

Date presented to CPWG:	September 20, 2011
Date presented to FPKIPA:	October 18, 2011
Date of approval by FPKIPA:	October 18, 2011