FBCA Certificate Policy Change Proposal Number: 2011-06

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Proposed modifications to the FBCA 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 Federal Bridge Certification Authority (FBCA)*; and 2) *FPKI X.509 Certificate and CRL Extensions Profile*

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 of *X.509 Certificate Policy for the FBCA* will be updated to remove the requirement for LDAP support. The new text will require support for any URI asserted in a valid certificate issued under the FBCA Certificate Policy, and the new text will not name any specific protocols. In addition, sections 4.3.1, 5.1.3, 5.7.4, 6.1.4, and 6.7 of the FBCA Certificate Policy will also be updated to change "directory" references to "repository" references.

FPKI X.509 Certificate and CRL Extensions Profile 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 *FPKI X.509 Certificate and CRL Extensions Profile* worksheets will be updated:

- Worksheet 1: Self-Signed CA Certificate Profile
- Worksheet 2: Key Rollover CA Certificate Profile
- Worksheet 3: Cross-Certificate Profile
- Worksheet 5: End-Entity Signature Certificate Profile
- Worksheet 6: Key Management Certificate Profile

Specific Changes:

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

X.509 Certificate Policy for the FBCA

2.1.1 FBCA Repository Obligations

The FPKI Management Authority may use a variety of mechanisms for posting information into a repository as required by this CP. These mechanisms at a minimum shall include:

- ~~X.500 Directory Server System that is also accessible through the Lightweight Directory Access Protocol,~~X.500 Directory Server System that is optionally accessible through the Lightweight Directory Access Protocol

  [Practice Note: The X.500 Directory Server System supporting LDAP will remain available until such time as the FPKIMA has determined that the Federal PKI community no longer requires Directory System Protocol (DSP).]

- Availability of the information as required by the certificate information posting and retrieval stipulations of this CP, and
- Access control and communication mechanisms when needed to protect repository information as described in later sections.

2.2.1 Publication of Certificates and Certificate Status

CA and End Entity certificates shall only contain valid Uniform Resource Identifiers (URIs) that are accessible by relying parties.

The FPKI Management Authority shall publish all CA certificates issued by or to the FBCA and all CRLs issued by the FBCA in the FBCA repository.

At a minimum, the Entity repositories shall contain all CA certificates issued by or to the Entity PKI and CRLs issued by the Entity PKI.

For the FBCA, mechanisms and procedures shall be designed to ensure CA certificates and CRLs are available for retrieval 24 hours a day, 7 days a week, with a minimum of 99% availability overall per year and scheduled down-time not to exceed 0.5% annually.

Entity CAs being considered for cross certification shall be designed to comply with this requirement.

4.3.1 CA Actions during Certificate Issuance

The FPKI Management Authority verifies the source of a certificate request before issuance. CA certificates created by the FBCA shall be checked to ensure that all fields and extensions are properly populated. After generation and verification, the FPKI Management Authority shall post CA certificates in the FBCA ~~directory~~ repository system.

5.1.3 Power and Air Conditioning

The FBCA and Entity CAs (operating at the Basic Assurance level or higher) shall have backup capability sufficient to automatically lock out input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. In addition, the FBCA ~~directories~~ repositories (containing FBCA issued certificates and CRLs) shall be provided with Uninterrupted Power sufficient for a minimum of six hours operation in the absence of commercial power. Entity CAs shall employ appropriate mechanisms to ensure availability of repositories as specified in Section 2.2.1.

5.7.4 Business Continuity Capabilities after a Disaster

The FBCA ~~directory~~ repository system shall be deployed so as to provide 24 hour, 365 day per year availability. The FPKI Management Authority shall implement features to provide high levels of ~~directory~~ repository reliability.

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 should be distributed using ~~directories and other~~ repositories.

6.7 NETWORK SECURITY CONTROLS

Network security controls shall be employed to protect the FBCA and the FBCA ~~Internal Directory~~ repository. Networking equipment shall turn off unused network ports and services. Any network software installed on the FBCA equipment shall be necessary to the functioning of the FBCA.

The FBCA ~~Border Directory~~ repository shall be connected to the Internet and provide continuous service (except, when necessary, for brief periods of maintenance or backup).

Any boundary control devices used to protect the ~~Border Directory~~ FBCA repository or FBCA local area network shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

Entity CAs, RAs, CMSs, ~~directories~~ repositories, remote workstations used to administer the CAs, and certificate status servers 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.

FPKI X.509 Certificate and CRL Extensions Profile

Worksheet 1: Self-Signed CA Certificate Profile

subjectInfoAccess			
accessMethod		id-ad-caRepository (1.3.6.1.5.5.7.48.5)	All CA certificates must include at least one instance of this access method that uses the URI name form to specify the location of an ~~LDAP~~ HTTP accessible ~~directory~~ server where CA certificates issued by the subject of this certificate may be found. CA certificates may also include an instance of this access method that uses the URI

			name form to specify the location of an ~~HTTP~~ LDAP accessible ~~Web~~ directory server.

Worksheet 2: Key Rollover CA Certificate Profile

cRLDistributionPoints	FALSE		This extension must appear in all certificates and must include at least an ~~LDAP~~ HTTP URI distribution point name. This profile recommends against the use of indirect CRLs or CRLs segmented by reason code.
authorityInfoAccess			
accessMethod		id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	All certificates must include at least one instance of this access method that uses the URI name form to specify the location of an ~~LDAP~~HTTP accessible ~~directory~~ server where certificates issued to the issuer of this certificate may be found. Certificates may also include an instance of this access method that uses the URI name form to specify the location of an ~~HTTP~~LDAP accessible ~~Web~~ directory server.
subjectInfoAccess			
accessMethod		id-ad-caRepository (1.3.6.1.5.5.7.48.5)	All CA certificates must include at least one instance of this access method that uses the URI name form to specify the location of an ~~LDAP~~ HTTP accessible ~~directory~~ server where CA certificates issued by the subject of this certificate

			may be found. CA certificates may also include an instance of this access method that uses the URI name form to specify the location of an ~~HTTP~~ LDAP accessible ~~Web~~ directory server.

Worksheet 3: Cross-Certificate Profile

cRLDistributionPoints	FALSE		This extension must appear in all certificates and must include at least an ~~LDAP~~ HTTP URI distribution point name. This profile recommends against the use of indirect CRLs or CRLs segmented by reason code.
authorityInfoAccess			
accessMethod		id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	All certificates must include at least one instance of this access method that uses the URI name form to specify the location of an ~~LDAP~~HTTP accessible ~~directory~~ server where certificates issued to the issuer of this certificate may be found. Certificates may also include an instance of this access method that uses the URI name form to specify the location of an ~~HTTP~~LDAP accessible ~~Web~~ directory server.
subjectInfoAccess			
accessMethod		id-ad-caRepository (1.3.6.1.5.5.7.48.5)	All CA certificates must include at least one instance of this access method that uses the URI name form to specify the location of an

			~~LDAP~~ HTTP accessible ~~directory~~ server where CA certificates issued by the subject of this certificate may be found. CA certificates may also include an instance of this access method that uses the URI name form to specify the location of an ~~HTTP~~ LDAP accessible ~~Web~~ directory server.

Worksheet 5: End-Entity Signature Certificate Profile

cRLDistributionPoints	FALSE		This extension must appear in all certificates and must include at least an ~~LDAP~~ HTTP URI distribution point name. This profile recommends against the use of indirect CRLs or CRLs segmented by reason code.
authorityInfoAccess			
accessMethod		id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	All certificates must include at least one instance of this access method that uses the URI name form to specify the location of an ~~LDAP~~HTTP accessible ~~directory~~ server where certificates issued to the issuer of this certificate may be found. Certificates may also include an instance of this access method that uses the URI name form to specify the location of an ~~HTTP~~LDAP accessible ~~Web~~ directory server.

Worksheet 6: Key Management Certificate Profile

cRLDistributionPoints	FALSE		This extension must appear in all certificates and must include at least an ~~LDAP~~ HTTP URI distribution point name. This profile recommends against the use of indirect CRLs or CRLs segmented by reason code.
authorityInfoAccess			
accessMethod		id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	All certificates must include at least one instance of this access method that uses the URI name form to specify the location of an ~~LDAP~~HTTP accessible ~~directory~~ server where certificates issued to the issuer of this certificate may be found. Certificates may also include an instance of this access method that uses the URI name form to specify the location of an ~~HTTP~~LDAP accessible ~~Web~~ directory server.

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 FBCA 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