



Federal Bridge CA Certificate Policy Change Proposal
Change Number: 2004-01

To: Federal PKI Policy Authority
From: FPKI Certificate Policy Working Group
Subject: Proposed modifications to the Common Certificate Policy
Date: 8 June 2004
Title: Common Policy Modifications and Clarifications

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy for the Common Policy Framework, February 10, 2004.

Change Advocates Contact Information:

Name: Tim Polk
Organization: NIST
Telephone number: 301-975-3348
E-mail address: tim.polk@nist.gov

Organization requesting change: Shared Service Provider Subcommittee

Change summary: The CPWG is proposing changes in the Common Policy to support the SSP process and assist agencies that are implementing the Common Policy.

Background: The CPWG met on 21 May 2004 to discuss issues raised by prospective Shared Service Providers during the process of establishing a Certified Providers List.

Specific Changes:

Specific changes are made to section 3.1.1, 4.4.3.1, 6.1.9, 6.2.4.1, 7.1 and 9. Deleted text is shown with strikethrough; inserted text is underlined:

Issue #1

Issue #1 Summary: To achieve name uniqueness, SSPs have stated requirements for multi-valued RDNs and inclusion of serial number and user id attributes within the subject name.

Section 3.1.1 Types of Names

The CA shall assign X.500 distinguished names to all subscribers. These distinguished names may be in either of two forms: an X.501 distinguished name specifying a geo-political name; and an Internet domain component name.

All geo-political X.501 distinguished names assigned to federal employees shall be in one of the following directory information trees:

C=US, o=U.S. Government, [ou=department], [ou=agency]
C=US, [o=department], [ou=agency]

New implementations shall assign names in the following directory tree:

C=US, o=U.S. Government, [ou=department], [ou=agency]

The organizational units *department* and *agency* appear when applicable and are used to specify the federal entity that employs the subscriber. At least one organizational unit must appear in the DN. The distinguished name of the federal employee subscriber will take one of the four following forms:

- C=US, o=U.S. Government, [ou=department], [ou=agency], cn=*nickname lastname*
- C=US, o=U.S. Government, [ou=department], [ou=agency], cn=*firstname initial. lastname*
- C=US, o=U.S. Government, [ou=department], [ou=agency], cn=*firstname middlename lastname*
- ~~C=US, o=U.S. Government, [ou=department], [ou=agency], cn=*firstname middlename lastname*, dnQualifier=*integer*~~

In the first name form, *nickname* may be the subscriber's first name, a form of the first name, middle name, or pseudonym (e.g., Buck) by which the subscriber is generally known. ~~In the last form, dnQualifier is an integer value that makes the name unique. The last form shall be used only if the other three name forms have already been assigned to subscribers.~~

X.501 distinguished names assigned to federal contractors and other affiliated persons shall be within the same directory information tree. The distinguished name of the federal contractor subscribers and affiliate subscribers will take one of the four following forms:

- C=US, o=U.S. Government, [ou=department], [ou=agency], cn=*nickname lastname (affiliate)*
- C=US, o=U.S. Government, [ou=department], [ou=agency], cn=*firstname initial. lastname (affiliate)*
- C=US, o=U.S. Government, [ou=department], [ou=agency], cn=*firstname middlename lastname (affiliate)*
- ~~C=US, o=U.S. Government, [ou=department], [ou=agency], cn=*firstname middlename lastname (affiliate)*, dnQualifier=*integer*~~

Legacy implementations which predate this policy may use the directory tree:

C=US, [o=department], [ou=agency]

Common name fields shall be populated as specified above.

Distinguished names based on Internet domain component names shall be in the following directory information trees:

dc=gov, dc=org0, [dc=org1],...[dc=orgN]

dc=mil, dc=org0, [dc=org1],...[dc=orgN]

The default Internet domain name for the agency, [orgN]...[org0].gov or [orgN]...[org0].mil will be used to determine DNs. The first domain component of the DN will either be dc=gov or dc=mil. At least, the org0 domain component must appear in the DN. The org1 to orgN domain components appear, in order, when applicable and are used to specify the federal entity that employs the subscriber.

The distinguished name of the federal employee subscriber may take one of the four following forms when their agency's Internet domain name ends in .gov:

- dc=gov, dc=org0, [dc=org1], ...[dc=orgN], cn=nickname lastname
- dc=gov, dc=org0, [dc=org1],...[dc=orgN], cn=firstname initial. lastname
- dc=gov, dc=org0, [dc=org1],...[dc=orgN], cn=firstname middlename lastname
- ~~dc=gov, dc=org0, [dc=org1],...[dc=orgN], cn=firstname middlename lastname, dnQualifier=integer~~

The distinguished name of the federal contractors and affiliated subscribers may take one of the four following forms when the agency's Internet domain name ends in .gov:

- dc=gov, dc=org0, [dc=org1],...[dc=orgN], cn=nickname lastname (affiliate)
- dc=gov, dc=org0, [dc=org1],...[dc=orgN], cn=firstname initial. lastname (affiliate)
- dc=gov, dc=org0, [dc=org1],...[dc=orgN], cn=firstname middlename lastname (affiliate)
- ~~dc=gov, dc=org0, [dc=org1],...[dc=orgN], cn=firstname middlename lastname (affiliate); dnQualifier=integer~~

The distinguished name of the federal employee subscriber may take one of the four following forms when their agency's Internet domain name ends in .mil:

- dc=mil, dc=org0, [dc=org1], ...[dc=orgN], cn=nickname lastname
- dc=mil, dc=org0, [dc=org1],...[dc=orgN], cn=firstname initial. lastname
- dc=mil, dc=org0, [dc=org1],...[dc=orgN], cn=firstname middlename lastname
- ~~dc=mil, dc=org0, [dc=org1],...[dc=orgN], cn=firstname middlename lastname, dnQualifier=integer~~

The distinguished name of the federal contractors and affiliated subscribers may take one of the four following forms when the agency's Internet domain name ends in .mil:

- dc=mil, dc=org0, [dc=org1],...[dc=orgN], cn=nickname lastname (affiliate)
- dc=mil, dc=org0, [dc=org1],...[dc=orgN], cn=firstname initial. lastname (affiliate)
- dc=mil, dc=org0, [dc=org1],...[dc=orgN], cn=firstname middlename lastname (affiliate)
- ~~dc=mil, dc=org0, [dc=org1],...[dc=orgN], cn=firstname middlename lastname (affiliate); dnQualifier=integer~~

The CA may supplement any of the name forms for users specified in this section by including a dnQualifier, serial number, or user id attribute. When any of these attributes are included, they may appear as part of a multi-valued RDN with the common name or as a distinct attribute.

Devices that are the subject of certificates issued under this policy may be assigned either a geo-political name or an Internet domain component name. Device names may take the following forms:

- C=US, o=U.S. Government, [ou=department], [ou=agency], cn=device name
- dc=gov, dc=org0, [dc=org1], ...[dc=orgN], [cn=device name]

· dc=mil, dc=org0, [dc=org1], ...[dc=orgN], [cn=device name]

where *device name* is a descriptive name for the device. Where a device is fully described by the Internet domain name, the common name attribute is optional.

This policy does not restrict the directory information tree for names of CAs. However, CAs that issue certificates under this policy must have distinguished names. CA distinguished names may be either a geo-political name or an Internet domain component name.

CA geo-political distinguished names may be composed of any combination of the following attributes: country; organization; organizational unit; and common name. Internet domain component names are composed of the following attributes: domain component; and common name.

Issue #2:

Summary: The Common Certificate Policy Framework imposed requirements for CRL issuance frequency of 24 hours. The authors assumed that the CRL expiration would match this frequency requirement. However, some SSP vendors have interpreted this text as permitting radically different CRL expiration times (e.g., one week). The following change clarifies the CPWG's intent.

4.4.3.1 CRL Issuance Frequency

CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below.

Certificate status information shall be published not later than the next scheduled update. This will facilitate the local caching of certificate status information for offline or remote (laptop) operation.

CAs shall make public a description of how to obtain revocation information for the certificates they publish, and an explanation of the consequences of using dated revocation information. This information shall be given to subscribers during certificate request or issuance, and shall be readily available to any potential relying party.

CAs that only issue certificates to CAs and that operate offline must issue CRLs at least once every 24 hours, and the *nextUpdate* time in the CRL may be no later than 24 hours after issuance time (i.e., the *thisUpdate* time). CAs that issue certificates to subscribers or operate online must issue CRLs at least once every 18 hours, and the *nextUpdate* time in the CRL may be no later than 18 hours after issuance time (i.e., the *thisUpdate* time). When a CA certificate is revoked because of compromise, or suspected compromise, of a private key, a CRL must be issued within 6 hours of notification.

Issue #3:

Summary: The Common Certificate Policy did not permit dual use certificates. Device certificates need to support both signature and key transport to implement significant protocols (e.g., TLS). This change explicitly permits dual use certificates for devices.

6.1.9 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The use of a specific key is constrained by the key usage extension in the X.509 certificate.

Public keys that are bound into subscriber user certificates shall be used only for signing or encrypting, but not both. User cCertificates to be used for digital signatures (including authentication) shall assert the *digitalSignature* and/or *nonRepudiation* bits. User cCertificates to be used for key transport shall assert the *keyEncipherment* bit.

Public keys that are bound into CA certificates shall be used only for signing certificates and status information (e.g., CRLs). CA certificates whose subject public key is to be used to verify other certificates shall assert the *keyCertSign* bit. CA certificates whose subject public key is to be used to verify CRLs shall assert the *cRLSign* bit. If the CA certificate is to be used to verify both certificate and CRLs, both the *keyCertSign* and *cRLSign* bits shall be asserted.

Public keys that are bound into device certificates may be used for signing, encrypting, or both. Device certificates to be used for digital signatures (including authentication) shall assert the *digitalSignature* bit. Device certificates to be used for key transport shall assert the *keyEncipherment* bit.

The *dataEncipherment*, *encipherOnly*, and *decipherOnly* bits shall not be asserted in certificates issued under this policy.

Issue #4:

Summary: The Common Certificate Policy restricts the CA to, at most, two backup copies of the private key. An applicant for the SSP program would like to maintain additional backup copies, as they maintain multiple hot sites. This change would permit CAs to maintain additional copies as long as the location is known for every key and the keys are protected as strongly as the original key.

6.2.4.1 Backup of CA Private Signature Key

The CA private signature keys shall be backed up under the same multiperson control as the original signature key. All copies of the CA private signature key shall be accountable material, and protected in the same manner as the original. ~~Such backup shall create only a single copy of the signature key at the CA location; a second copy may be kept at the CA backup location.~~ Backup procedures shall be included in the CA's CPS.

Issue #5:

Summary: The Common CP Certificate Profile was intended to apply to SSPs, not agencies that also support the Common Policy. This requirement can be enforced by the SSP Subcommittee during the Certified Providers List process. The Federal Certificate Profile is a superset of the Common CP Certificate Profile, and reflects the requirements on federal agency PKIs.

7.1 Certificate Profile

Certificates issued by a CA under this policy shall conform to the Common CP Federal Public Key Infrastructure X.509 Certificate and CRL Extensions Profile [FPKI-PROF][CCP-PROF].

9. Bibliography

~~CCP-Prof X.509 Certificate and CRL Extensions Profile for the Common Policy, December 8, 2003. .~~

FPKI-PROF

Federal Public Key Infrastructure X.509 Certificate and CRL Extensions Profile.

Estimated Cost:

There is no cost associated with this CP change.

Implementation Date:

This change will be implemented immediately upon approval by the FPKIPA and incorporation into the SSP review procedures.

Prerequisites for Adoption:

There are no prerequisites.

Plan to Meet Prerequisites:

There are no prerequisites.

Approval and Coordination Dates:

Date presented to CPWG:	21 May 2004
Date CPWG recommended approval:	21 May 2004
Date Presented to FPKI PA:	8 June 2004
Date of approval by FPKI PA:	13 July 2004