Common Policy Change Proposal Number: 2007-02

To:	**Federal PKI Policy Authority**
From:	Certificate Policy Working Group
Subject:	Proposed modifications to the Common Certificate Policy
Date:	September 12, 2007
Title:	Requiring the inclusion of a subject DN in PIV Authentication Certificates

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 3647 – 1.1, August 16, 2007.

Change Advocate's Contact Information:

Name: David Cooper
Organization: NIST
Telephone number: 301-975-3194
E-mail address: david.cooper@nist.gov

Organization requesting change: Federal PKI Policy Authority

Change summary: The Common Policy currently states that certificates issued under id-fpki-common-authentication may optionally include a subject DN if the subject DN is populated following the same rules as for certificates issued under id-fpki-common-hardware. This change proposal requests that the requirements for certificates issued under id-fpki-common-authentication be modified to require the inclusion of a non-empty subject DN. The subject DN could be populated either following the rules for subject DNs in certificates issued under id-fpki-common-hardware or following the rules for including non-empty subject DNs in certificates issued under id-fpki-common-cardAuth.

Background: The current policy for issuing PIV Authentication certificates under id-fpki-common-authentication satisfies almost all of the requirements for FBCA Medium Hardware. However, all policies in the FBCA CP except Rudimentary require the inclusion of a non-empty subject DN in all certificates, whereas the Common Policy makes the inclusion of a subject DN in certificates issued under id-fpki-common-authentication optional. This disconnect prevents relying parties that do not use the Common Policy Root CA as a trust anchor from recognizing certificates issued under id-fpki-common-authentication at an assurance level higher than Rudimentary. This change proposal would result in relying parties that do not use the Common Policy Root CA as a trust anchor being able to recognize certificates issued under id-fpki-common-authentication as satisfying FBCA Medium Hardware.

Specific Changes: Specific changes are made to the following sections: 1.4.1, 3.1.1, and 7.1.4

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

1.4.1 Appropriate Certificate Uses

Modify the third paragraph of section 1.4.1 as follows:

Credentials issued under the id-fpki-common-policy ~~and id-fpki-common-authentication~~ policy~~ies~~ are intended to meet the requirements for Level 3 authentication, as defined by the OMB E-Authentication Guidance. [E-Auth] Credentials issued under the id-fpki-common-hardware, id-fpki-common-authentication, and id-fpki-common-High policies meet the requirements for Level 4 authentication, as defined by the OMB E-Authentication Guidance. [E-Auth]

3.1.1 Types of Names

Modify the second to last paragraph of section 3.1.1 as follows:

For certificates issued under id-fpki-common-authentication, assignment of X.500 distinguished names is mandatory~~optional~~. ~~If assigned, d~~Distinguished names shall follow either the rules specified above for id-fpki-common-hardware or the rules specified below for including a non-NULL subject DN in id-fpki-common-cardAuth. Certificates issued under id-fpki-common-authentication shall include a subject alternative name. At a minimum, the subject alternative name extension shall include the pivFASC-N name type [FIPS 201-1]. The value for this name shall be the FASC-N [PACS] of the subject's PIV card.

7.1.4 Name Forms

Modify the first paragraph of section 7.1.4 as follows:

The subject field in certificates issued under id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-authentication, id-fpki-common-High, and id-fpki-common-devices ~~of the base certificate~~ shall be populated with an X.500 distinguished name as specified in section 3.1.1.

Estimated Cost:

No cost to the Common Policy Root CA.

Risk/Impact:

This change would not lower the assurance level of any certificates issued under the Common Policy.

Implementation Date:

This change will be implemented immediately upon approval by the FPKIPA and incorporation into the Common Certificate Policy.

Prerequisites for Adoption:

There are no prerequisites.

Plan to Meet Prerequisites:

There are no prerequisites.

Approval and Coordination Dates:

Date presented to CPWG: August 21, 2007
Date presented to FPKI PA: September 21, 2007
Date of approval by FPKI PA: October 2, 2007