



Common Policy Change Proposal Number: 2010-03

To: Federal PKI Policy Authority
From: Certificate Policy Working Group
Subject: Proposed modifications to the Common Certificate Policy
Date: March 4, 2010
Title: Allowing inclusion of UUIDs in Card 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 – 1.8, 1/21/2010.

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: This change proposal aligns the Common Certificate Policy with NIST SP 800-73-3 by permitting Card Authentication certificates to include Universal Unique Identifiers (UUID).

Background: Since the Card Authentication certificate is available for free read over the contactless interface, the Common Certificate Policy strictly limits the amount of identifying information that may be included in these certificates. Currently, the only name form that the Common Certificate Policy permits to appear in Card Authentication certificates is the FASC-N.

Since the FASC-N namespace is limited to Federal government card issuers, NIST SP 800-73-3 introduces the UUID as an alternative namespace for use in PIV Compatible and PIV Interoperable cards, and permits the use of UUIDs in PIV cards in addition to the FASC-N. Due to the way that UUIDs are constructed, inclusion of a UUID in a certificate provides no additional identifying information about the certificate subject.

NIST SP 800-73-3 indicates that when PIV card issuers choose to include UUIDs on PIV Cards, the UUID should appear in both the PIV Authentication certificate and the Card Authentication certificate. This change proposal aligns the Common Certificate Policy with NIST SP 800-73-3 by permitting certificates issued under id-fpki-common-cardAuth to include UUIDs. Since the Common Certificate Policy does not limit the set of name forms that may appear in certificates

issued under id-fpki-common-authentication, no changes are required to the Common Certificate Policy to permit the inclusion of UUIDs in PIV Authentication certificates.

Specific Changes: Specific changes are made to the following sections: 3.1.1, 10, and 11

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

3.1.1 Types of Names

Modify the final paragraph of section 3.1.1 as follows:

Certificates issued under id-fpki-common-cardAuth shall include a subject alternative name extension that includes the pivFASC-N name type. The value for this name shall be the FASC-N of the subject's PIV card. Certificates issued under id-fpki-common-cardAuth may also include a UUID [RFC 4122] in the subject alternative name extension, if the UUID is included as specified in Section 3.3 of [SP 800-73-3(1)]. Certificates issued under id-fpki-common-cardAuth shall not include any other name in the subject alternative name extension but may include a non-NULL name in the subject field. If included, the subject distinguished name shall take one of the following forms:

- C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structural_container], serialNumber=FASC-N
- dc=gov, dc=org0, [dc=org1], ..., [dc=orgN], [ou=structural_container], serialNumber=FASC-N
- dc=mil, dc=org0, [dc=org1], ..., [dc=orgN], [ou=structural_container], serialNumber=FASC-N
- C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structural_container], serialNumber=UUID
- dc=gov, dc=org0, [dc=org1], ..., [dc=orgN], [ou=structural_container], serialNumber=UUID
- dc=mil, dc=org0, [dc=org1], ..., [dc=orgN], [ou=structural_container], serialNumber=UUID

Practice Note: The FASC-N [PACS] consists of 40 decimal digits that are encoded as a 25-byte binary value. This 25-byte binary value may be encoded directly into the pivFASC-N name type in the subject alternative name extension, but when included in the subject field the FASC-N must be encoded as a PrintableString that is at most 64 characters long. This policy does not mandate any particular method for encoding the FASC-N within the serial number attribute as long as the same encoding method is used for all certificates issued by a CA. Acceptable methods for encoding the FASC-N within the serial number attribute include encoding the 25-byte binary value as 50 bytes of ASCII HEX or encoding the 40 decimal digits as 40 bytes of ASCII decimal.

Practice Note: <u>When the UUID appears in the subjectAltName extension of a certificate, it must be encoded as a uniformResourceIdentifier as specified in Section 3 of [RFC 4122]. An example of a UUID encoded as a URI, from RFC 4122, is "urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6". This policy does not mandate any particular method for encoding the UUID within the serial number attribute as long as the same encoding method is used for all certificates issued by the CA and it is encoded as a PrintableString that is at most 64 characters long, however, it is recommended that the string representation from Section 3 of [RFC 4122] be used. An example would be "f81d4fae-7dec-11d0-a765-00a0c91e6bf6".</u>

10. Bibliography

Add the following bibliography entries:

- RFC 4122 A Universally Unique IDentifier (UUID) URN Namespace, Paul J. Leach, Michael Mealling, and Rich Salz, July 2005.
<http://www.ietf.org/rfc/rfc4122.txt>
- SP 800-73-3(1) Interfaces for Personal Identity Verification – Part 1: End-Point PIV Card Application Namespace, Data Model and Representation, NIST Special Publication 800-73-3, February 2010.

11. Acronyms and Abbreviations

Add the following acronym:

UUID Universal Unique Identifier

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: October 20, 2009
Date Presented to FPKIPA March 9, 2010
Date of approval by FPKIPA: March 9, 2010