Common Policy Framework Certificate Policy Change Proposal Number: 2012-05

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Proposed modifications to the Common Policy Framework Certificate Policy
Date: October 4, 2012

Title: Common PIV Content Signing Policy OID

Version and Date of Certificate Policy Requested to be changed: X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, Version 1.19, June 22, 2012

Change Advocate's Contact Information: CPWG

Organization requesting change: FPKI Certificate Policy Working Group

Change summary: Implementation of this change proposal will create a new Common PIV Content Signing Policy OID in the Common Policy

Background:

Currently, FIPS 201-2 revised draft requires the id-fpki-common-devicesHardware, id-fpki-common-hardware, or id-fpki-common-High policy OID plus the PIV Content Signing EKU for certificates issued to PIV card issuing systems for signing content encoded on PIV cards. NIST stated they would reference a Common PIV Content Signing Policy OID in FIPS 201 if it were included in the Common Policy. The CPWG has recommended to NIST that FIPS 201-2 should simply reference the Common Policy for all technical specifications related to PKI. However, the Common PIV Content Signing Policy should be defined in the Common Policy in time for FIPS 201 to reference it, in case the FPKIPA recommendation, to reference Common Policy for technical PKI specifications in FIPS 201, is not accepted.

Adding this policy OID provides a strong mechanism to strengthen Common Policy requirements for PIV identity and biometric content signing and it aligns with PIV-I policy in the FBCA requirements (which was developed using lessons learned from PIV). In addition, it provides specific requirements for certificates issued to card issuing systems that are used to sign the identity and biometric content encoded on PIV cards. Content signing operations must be conformant with PIV issuance requirements. Other benefits are that more applications currently process policy OIDs than EKUs. This policy

OID will provide a critical link for relying parties in establishing the integrity of identity data which originates from PIV.

The FPKIPA must consider the following when implementing this change

- SSPs will need new certificates to add in this policy
- SSPs (and Federal Issuers) will need to weigh in on cost to implement
- There will be a transition period
- Impact is limited – small number of PIV Issuers – which is the main focus of the change

Overall, the benefits of this change outweigh the additional effort required for implementation.

Specific Changes:

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

1.2 DOCUMENT IDENTIFICATION

Table 1 - id-fpki-common Policy OIDs

id-fpki-common-policy	::= {2 16 840 1 101 3 2 1 3 6}
id-fpki-common-hardware	::= {2 16 840 1 101 3 2 1 3 7}
id-fpki-common-devices	::= {2 16 840 1 101 3 2 1 3 8}
id-fpki-common-devicesHardware	::= {2 16 840 1 101 3 2 1 3 36}
id-fpki-common-authentication	::= {2 16 840 1 101 3 2 1 3 13}
id-fpki-common-High	::= {2 16 840 1 101 3 2 1 3 16}
id-fpki-common-cardAuth	::= {2 16 840 1 101 3 2 1 3 17}
id-fpki-common-piv-contentSigning	::= {2 16 840 1 101 3 2 1 3 39}

…..

This document includes ~~two~~three policies specific to the FIPS 201 Personal Identity Verification Card. Certificates issued to users supporting authentication but not digital signature may contain id-fpki-common-authentication. Certificates issued to users supporting authentication where the private key can be used without user authentication may contain id-fpki-common-cardAuth. The id-fpki-common-piv-contentSigning policy shall only be asserted in certificates issued to devices that sign PIV Card objects in accordance with [FIPS 201].

The requirements associated with id-fpki-common-piv-contentSigning are identical to id-fpki-common-devicesHardware except where specifically noted in the text.

1.4.1 Appropriate Certificate Uses

Credentials issued under the id-fpki-common-policy policy 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]

Credentials issued under the id-fpki-common-piv-contentSigning policy are intended to meet the requirements in FIPS 201 as the digital signatory of the PIV Card Holder Unique IDentifier (CHUID) and associated PIV card objects.

3.1.1 Types of Names

CA and CSS geo-political distinguished names shall 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; organizational unit; and common name.

The Common PIV Content Signing certificate's subject DN shall indicate the organization administering the PIV card issuance system or device according to types of names for devices.

For certificates issued under id-fpki-common-authentication, assignment of X.500 distinguished names is mandatory.

6.1.1.4 PIV Content Signing Key Pair Generation

Cryptographic keying material used by PIV card issuing systems or devices for Common PIV Content Signing shall be generated in FIPS 140 validated cryptographic modules. For PIV card issuing systems or devices that sign PIV objects on PIV cards that contain certificates that assert id-fpki-common-High, the module(s) shall meet or exceed FIPS 140 Level 3. For all other PIV card issuing systems or devices, the module(s) shall meet or exceed FIPS 140 Level 2. Key generation procedures shall be documented.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

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

Signing certificates issued under the policy for id-fpki-common-piv-contentSigning shall include an extended key usage of *id-PIV-content-signing* (see [CCP-PROF]).

6.2.4.6 Backup of Common PIV Content Signing Key

The Common PIV Content Signing private signature keys shall be backed up under multi-person control. At least one copy of the private signature key shall be stored in a secondary location. All copies of the Common PIV Content Signing private signature key shall be accounted for and protected in the same manner as the original. Backed up Common PIV Content private signature keys shall not be exported or stored in plaintext form outside the cryptographic module. Backup procedures shall be documented.

6.2.8 Method of Activating Private Keys

For certificates issued under id-fpki-common-devices and id-fpki-common-devicesHardware, the device may be configured to activate its private key without requiring its human sponsor or authorized administrator to authenticate to the cryptographic token, provided that appropriate physical and logical access controls are implemented for the device and its cryptographic token. For certificates issued under id-fpki-common-piv-contentSigning, the PIV card issuance system or device may be configured to activate its private key without requiring its human sponsor or authorized administrator to authenticate to the cryptographic token, provided that appropriate physical and logical access controls are implemented for content signing operations conformant with PIV issuance requirements (see [FIPS 201]). The strength of the security controls shall be commensurate with the level of threat in the device's environment, and shall protect the device's hardware, software, and the cryptographic token and its activation data from compromise.

6.3.2 Certificate Operational Periods/Key Usage Periods

Subscriber public keys in certificates that assert the id-PIV-content-signing OID in the extended key usage extension have a maximum usage period of ~~eight~~nine years. The private keys corresponding to the public keys in these certificates have a maximum usage period of three years. Expiration of the id-fpki-common-piv-contentSigning certificate shall be later than the expiration of the id-fpki-common-authentication certificate expiration.

7.1.4 Name Forms

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

7.1.6 Certificate Policy Object Identifier

Certificates issued under this CP shall assert at least one of the following OIDs in the certificate policies extension, as appropriate:

id-fpki-common-policy ::= {2 16 840 1 101 3 2 1 3 6}

id-fpki-common-hardware ::= {2 16 840 1 101 3 2 1 3 7}

id-fpki-common-devices ::= {2 16 840 1 101 3 2 1 3 8}

id-fpki-common-devicesHardware ::= {2 16 840 1 101 3 2 1 3 36}

id-fpki-common-authentication ::= {2 16 840 1 101 3 2 1 3 13}

id-fpki-common-High ::= {2 16 840 1 101 3 2 1 3 16}

id-fpki-common-cardAuth ::= {2 16 840 1 101 3 2 1 3 17}

id-fpki-common-piv-contentSigning ::= {2 16 840 1 101 3 2 1 3 39}

Certificates that express the id-fpki-common-piv-contentSigning policy OID, shall not express any other policy OIDs.

Estimated Cost: The estimated costs will be included in the cost of updating systems to comply with FIPS 201-2.

Implementation Date:

Implementation of this change will require transition planning, but will occur no later than 12 months after publication of FIPS 201-2.

Prerequisites for Adoption:

Before the requirements in this change proposal become mandatory, [CCP-PROF] will be updated and changes to FIPS 201-2 must be accepted and published.

Plan to Meet Prerequisites:

Not Applicable

Approval and Coordination Dates: *<These dates will be inserted by the CPWG>*

Date presented to CPWG:	2, 21 August 2012, 26 September 2012, 4 October 2012, 1 & 20 November 2012,
Date presented to FPKIPA:	October 16, 2012, November 6, 2012, December 4, 2012
Date of approval by FPKIPA:	