Common Policy Framework Certificate Policy Change Proposal Number: 2015-01

To: Federal PKI Policy Authority (FPKIPA)

From: Certificate Policy Working Group (CPWG)

Subject: Proposed modifications to the Common Policy Framework Certificate Policy

Date: April 2, 2015

Title: Common Derived PIV Authentication Certificate Policy OIDs

Version and Date of Certificate Policy Requested to be changed: X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, Version 1.23, May 5, 2014

Change Advocate's Contact Information: CPWG

Organization requesting change: FPKI Certificate Policy Working Group

Change summary: Implementation of this change proposal will create two new Common Derived PIV Authentication Certificate Policy OIDs in the Common Policy.

Background:

NIST Special Publication 800-157 introduces a new type of PIV credential, the X.509 Derived PIV Authentication certificate, which may be issued to PIV Card holders for use where use of a PIV Card is not practical. An X.509 Derived PIV Authentication certificate and its corresponding private key is issued in accordance with the requirements specified in SP 800-63-2 for derived credentials, and may be issued at either Level of Assurance 3 or 4. This change proposal introduces two new policy OIDs for these certificates, one for each assurance level.

Specific Changes:

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

FOREWORD

Modify the first paragraph as follows:

This is the policy framework governing the public key infrastructure (PKI) component of the Federal Enterprise Architecture. The policy framework incorporates ~~seven~~ ten specific certificate policies: a policy for users with software cryptographic modules, a policy for users

with hardware cryptographic modules, a policy for devices with software cryptographic modules, a policy for devices with hardware cryptographic modules, a policy for devices that sign PIV data objects, a high assurance user policy, ~~a~~ three user authentication policies~~policy~~, and a card authentication policy. There is one Certification Authority associated with the Common Policy Framework: The Federal Common Policy Root CA.

1. INTRODUCTION

Modify the first paragraph as follows:

This certificate policy (CP) includes ~~seven~~ ten distinct certificate policies: a policy for users with software cryptographic modules, a policy for users with hardware cryptographic modules, a policy for devices with software cryptographic modules, a policy for devices with hardware cryptographic modules, a policy for devices that sign PIV data objects, a high assurance user policy, ~~a~~ three user authentication policies ~~policy~~, and a card authentication policy. In this document, the term "device" means a non-person entity, i.e., a hardware device or software application. Where a specific policy is not stated, the policies and procedures in this specification apply equally to all ~~seven~~ ten policies.

1.2 DOCUMENT NAME AND IDENTIFICATION

This CP provides substantial assurance concerning identity of certificate subjects. Certificates issued in accordance with this CP and associated with the Federal Common Policy Root CA shall assert at least one of the following OIDs in the certificate policy extension:

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}
id-fpki-common-derived-pivAuth	::= {2 16 840 1 101 3 2 1 3 40}

id-fpki-common-derived-pivAuth-hardware	::= {2 16 840 1 101 3 2 1 3 41}

…

This document includes ~~three~~ five policies specific to ~~the~~ FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors ~~Card~~. Certificates issued to users supporting authentication but not digital signature, where the corresponding private key is stored on a PIV Card, may contain id-fpki-common-authentication. Certificates issued to users supporting authentication where the private key is stored on a PIV Card and can be used without user authentication may contain id-fpki-common-cardAuth. Certificates issued to users, in accordance with NIST SP 800-157, supporting authentication, but not digital signature, where the corresponding private key is not stored on a PIV Card, may contain either id-fpki-common-derived-pivAuth-hardware or id-fpki-common-derived-pivAuth as appropriate. The id-fpki-common-piv-contentSigning policy shall only be asserted in certificates issued to devices that sign PIV data ~~Card~~ objects in accordance with [FIPS 201] or [SP 800-157].

…

1.4.1 Appropriate Certificate Uses

Modify the third and fourth paragraphs as follows:

Credentials issued under the id-fpki-common-policy and id-fpki-common-derived-pivAuth policies ~~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, id-fpki-common-derived-pivAuth-hardware, 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 and SP 800-157 as the digital signatory of the PIV Card Holder Unique IDentifier (CHUID) and associated PIV ~~card~~ data objects.

3.1.1 Types of Names

Add the following as the second-to-last paragraph of Section 3.1.1:

Certificates issued under id-fpki-common-derived-pivAuth-hardware and id-fpki-common-derived-pivAuth shall include a non-empty subject DN and shall also include a subject alternative name extension that includes a UUID, which shall be encoded as a URI as specified in Section 3 of [RFC 4122]. A unique UUID shall be created for each certificate issued under one of these policies. For certificates issued under this policy by a CA operating as part of the Shared Service Providers program, subject 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 with a UUID in id-fpki-common-cardAuth. For legacy Federal PKIs only, distinguished names may follow established agency naming conventions.

Add a new section as follows:

3.2.3.3 Authentication for Derived PIV Credentials

For certificates issued under id-fpki-common-derived-pivAuth-hardware and id-fpki-common-derived-pivAuth, identity shall be verified in accordance with the requirements specified for issuing derived credentials in [SP 800-157]. The RA or CA shall:

1) Verify that the request for certificate issuance to the applicant was submitted by an authorized agency employee.

2) Use the PKI-AUTH authentication mechanism from Section 6 of FIPS 201 to verify that the PIV Authentication certificate on the applicant's PIV Card is valid and that the applicant is in possession of the corresponding private key.

3) Maintain a copy of the applicant's PIV Authentication certificate.

Seven days after issuing the Derived credential, the issuer should recheck the revocation status of the PIV Authentication certificate. This step can detect use of a compromised PIV Card to obtain a derived credential

For certificates issued under id-fpki-common-derived-pivAuth-hardware, the applicant shall appear at the RA in person to present the PIV Card and perform the PKI-AUTH authentication mechanism. The RA shall perform a one-to-one comparison of the applicant against biometric data stored on the PIV Card, in accordance with [SP 800-76], and shall record and maintain the biometric sample used to validate the applicant. In cases where a 1:1 biometric match against the biometrics available on the PIV Card or in the chain-of-trust, as defined in [FIPS201] is not possible:

i) The applicant shall present a government-issued form of identification (e.g., a passport or driver's license) in addition to the PIV Card, and

ii) The RA shall examine the presented credentials for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of the applicant), and

iii) The process documentation for the issuance of the certificate shall include the identity of the person performing the verification of the second (non-PIV) form of identification, a signed declaration by that person that he or she verified the identity of the applicant as required by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury), a unique identifying number from the second form of identification or a facsimile of the ID, a biometric of the applicant, and the date and time of the verification.

3.3.1 Identification and Authentication for Routine Re-key

CA certificate re-key shall follow the same procedures as initial certificate issuance.

For re-key of subscriber certificates issued under id-fpki-common-derived-pivAuth and id-fpki-

common-derived-pivAuth-hardware, the department or agency shall verify that the Subscriber is eligible to have a PIV Card (i.e., PIV Card is not terminated).

For re-key of subscriber certificates issued under id-fpki-common-High, identity may be established through use of current signature key, except that identity shall be established through an in-person registration process at least once every three years from the time of initial registration.

For policies other than id-fpki-common-High, a subscriber's identity may be established through use of current signature key, except that identity shall be re-established through an in-person registration process at least once every nine years from the time of initial registration.

In addition, for re-key of subscriber certificates issued under id-fpki-common-derived-pivAuth-hardware, identity shall be established via mutual authentication between the issuer and the cryptographic module containing the current key, if the new key will be stored in the same cryptographic module as the current key. Identity shall be established through the initial registration process if the new key will be stored in a different cryptographic module than the current key.

For device certificates, identity may be established through the use of the device's current signature key or~~,~~ the signature key of the device's human sponsor, except that identity shall be established through the initial registration process at least once every nine years from the time of initial registration.

4.9.9 On-line Revocation/Status Checking Availability

Modify the first paragraph as follows:

CAs shall support on-line status checking via OCSP [RFC 2560] for end entity certificates issued under id-fpki-common-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-derived-pivAuth, and id-fpki-common-cardAuth.

6.1.1.2 Subscriber Key Pair Generation

Modify the second paragraph as follows:

Validated software or hardware cryptographic modules shall be used to generate all subscriber key pairs, as well as pseudo-random numbers and parameters used in key pair generation. For the id-fpki-common-hardware, id-fpki-common-High, id-fpki-common-authentication, id-fpki-common-derived-pivAuth-hardware, and id-fpki-common-cardA~~a~~uth policies, subscriber key pairs shall be generated in FIPS 140 Level 2 hardware cryptographic modules. Any pseudo-random numbers used for key generation material shall be generated by a FIPS-approved method. Symmetric keys may be generated by means of either software or hardware mechanisms.

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.

6.1.5 Key Sizes

Modify the eighth paragraph as follows:

~~End entity certificates issued under id-fpki-common-authentication or id-fpki-common-cardAuth that expire before January 1, 2014 shall contain RSA public keys that are 1024 or 2048 bits in length or elliptic curve keys that are 256 bits.~~ End entity certificates issued under id-fpki-common-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-derived-pivAuth, or id-fpki-common-cardAuth ~~that expire on or after January 1, 2014~~ shall contain RSA public keys that are 2048 bits in length or elliptic curve keys that are 256 bits.

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

Modify the second paragraph as follows:

Public keys that are bound into subscriber user certificates shall be used only for signing or encrypting, but not both. User certificates that assert id-fpki-common-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-derived-pivAuth, or id-fpki-common-cardAuth shall only assert the *digitalSignature* bit. Other user certificates to be used for digital signatures shall assert both the *digitalSignature* and *nonRepudiation* bits. User certificates that contain RSA public keys that are to be used for key transport shall assert the *keyEncipherment* bit. User certificates that contain elliptic curve public keys that are to be used for key agreement shall assert the *keyAgreement* bit.

6.2.1 Cryptographic Module Standards and Controls

Modify the second paragraph as follows:

In accordance with FIPS 201, the relevant NIST Guideline for PIV Card Issuers (PCI) and Derived PIV Credential Issuers is NIST SP 800-79, Guidelines for the Accreditation of ~~Personal Identity Verification Card~~ PCIs and and Derived PIV Credential Issuers (DPCI), which utilizes various aspects of NIST SP 800-37 and applies them to accrediting the reliability of PCIs and DPCIs.

Modify the sixth paragraph as follows:

Subscribers shall use a FIPS 140 Level 1 or higher validated cryptographic module for all cryptographic operations. Subscribers issued certificates under the hardware users policy (id-fpki-common-hardware or id-fpki-common-devicesHardware), one of the hardware authentication policies (id-fpki-common-authentication, id-fpki-common-derived-pivAuth-hardware, or id-fpki-common-cardAuth), or common High policy (id-fpki-common-High) shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module for all private key operations.

6.2.4.2 Backup of Subscriber Private Signature Key

Subscriber private signature keys whose corresponding public key is contained in a certificate asserting the id-fpki-common-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-cardAuth, or id-fpki-common-High policy shall not be backed up or copied.

All other Subscriber private signature keys ~~whose corresponding public key is contained in a certificate that does not assert id-fpki-common-authentication, id-fpki-common-cardAuth, or id-fpki-common-High~~ may be backed up or copied, but must be held in the subscriber's control. Backed up subscriber private signature keys shall not be stored in plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.

6.2.8 Method of Activating Private Key

Modify the first paragraph as follows:

For certificates issued under id-fpki-common-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-derived-pivAuth, id-fpki-common-policy, id-fpki-common-hardware, and id-fpki-common-High, the subscriber must be authenticated to the cryptographic token before the activation of the associated private key(s). Acceptable means of authentication include but are not limited to passphrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

6.3.2 Certificate Operational Periods and Key Usage Periods

Modify the third paragraph as follows:

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 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, id-fpki-common-derived-pivAuth-hardware, or id-fpki-common-derived-pivAuth certificates ~~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-derived-pivAuth-hardware, id-fpki-common-derived-pivAuth, id-fpki-common-High, id-fpki-common-devices, id-fpki-common-devicesHardware, and id-fpki-common-piv-contentSigning shall be populated with an X.500 distinguished name as specified in section 3.1.1.

The issuer field of certificates issued under the policies in this document shall be populated with a non-empty X.500 Distinguished Name as specified in section 3.1.1.

The subject alternative name extension shall be present and include the pivFASC-N name type in certificates issued under id-fpki-common-authentication and id-fpki-common-cardAuth.

The subject alternative name extension shall be present and include a UUID, encoded as a URI, in certificates issued under id-fpki-common-authentication, id-fpki-common-cardAuth, id-fpki-common-derived-pivAuth-hardware and id-fpki-common-derived-pivAuth.

7.1.6 Certificate Policy Object Identifier

Modify the first paragraph as follows:

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-derived-pivAuth ::= {2 16 840 1 101 3 2 1 3 40}

id-fpki-common-derived-pivAuth-hardware ::= {2 16 840 1 101 3 2 1 3 41}

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}

BIBLIOGRAPHY

Modify the bibliography as follows:

FIPS 186-42 Digital Signature Standard (DSS), FIPS 186-42, July 2013~~January 27, 2000~~. ~~http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf~~ http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf

SP 800-37 Guide for Applying the Risk Management Framework to ~~Security Certification and Accreditation of~~ Federal Information Systems: A Security Life Cycle Approach, NIST Special Publication 800-37 Revision 1, February 2010 ~~May 2004~~. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf ~~http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf~~

SP 800-63 Electronic Authentication Guideline, NIST Special Publication 800-63-2, August 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

SP 800-76 Biometric Specifications for Personal Identity Verification, NIST Special Publication 800-76-2, July 2013.
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-76-2.pdf

SP 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials, NIST Special Publication 800-157.

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf or http://csrc.nist.gov/publications/drafts/800-157/sp800_157_draft.pdf

The following worksheet shall be added to the X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework:

Worksheet 11: Derived PIV Authentication Certificate Profile

Field	Criticality Flag	Value	**Comments**
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber		INTEGER	Unique positive integer.
signature			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field. The parameters field is only populated when the algorithm is RSA.
algorithm		Choice of following algorithms:	
		1.2.840.113549.1.1.10	id-RSASSA-PSS (RSA with PSS padding; 800-78 requires use with SHA-256 hash algorithm)
		1.2.840.113549.1.1.11	Sha256WithRSAEncryption
		1.2.840.10045.4.3.2	ecdsa-with-SHA256
		1.2.840.10045.4.3.3	ecdsa-with-SHA384
parameters		2.16.840.1.101.3.4.2.1	For id-RSASSA-PSS only, specify the SHA-256 hash algorithm as a parameter
		NULL	For all RSA algorithms except id-RSASSA-PSS
issuer			
Name			
RDNSequence			Must use one of the name forms specified in section 3.1.1 of the Common Certificate Policy.
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
validity			
notBefore			
Time			
utcTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
notAfter			The notAfter time MUST not be after the PIV card expiration date.
Time			
utcTime		YYMMDDHHMMSSZ	Use for dates up to and including 2049.
generalTime		YYYYMMDDHHMMSSZ	Use for dates after 2049
subject			
Name			X.500 Distinguished name of the owner of the certificate.
RDNSequence			Must use one of the name forms specified in section 3.1.1 of the Common Certificate Policy.

Field	Criticality Flag	Value	**Comments**
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
subjectPublicKeyInfo			
algorithm			
AlgorithmIdentifier			Public key algorithm associated with the public key. May be either RSA or elliptic curve.
algorithm		1.2.840.113549.1.1.1	RSA Encryption
		1.2.840.10045.2.1	Elliptic curve key
parameters			Format and meaning dependent upon algorithm
RSAParameters		NULL	For RSA, parameters field is populated with NULL.
EcpkParameters			
namedCurve		Implicitly specify parameters through an OID associated with a NIST approved curve referenced in 800-78:	
		1.2.840.10045.3.1.7	Curve P-256
subjectPublicKey		BIT STRING	
required extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
keyUsage	TRUE		Only digitalSignature shall be set.
digitalSignature		1	
nonRepudiation		0	
keyEncipherment		0	
dataEncipherment		0	
keyAgreement		0	
keyCertSign		0	
cRLSign		0	
encipherOnly		0	
decipherOnly		0	
certificatePolicies	FALSE		
PolicyInformation			Two policy OID are specified for PIV Derived Authentication certificates. Other policy OIDs may be asserted as well.
policyIdentifier		2.16.840.1.101.3.2.1.3.40	id-fpki-common-derived-pivAuth
		2.16.840.1.101.3.2.1.3.41	Id-fpki-common-derived-pivAuth-hardware
cRLDistributionPoints	FALSE		This extension is required in all end entity certificates and must contain an HTTP URL. The reasons and cRLIssuer fields must be omitted.
DistributionPoint			
distributionPoint			

Field	Criticality Flag	Value	**Comments**
DistributionPointName			
fullName			
GeneralNames			
GeneralName			
directoryName			
Name			
RDNSequence			
RelativeDistinguishedName			
AttributeTypeAndValue			
AttributeType		OID	
AttributeValue		see comment	See preamble text on naming.
uniformResourceIdentifier		ldap://… or http://…	See preamble text on URIs.
authorityInfoAccess	FALSE		authorityInfoAccess consists of a sequence of accessMethod and accessLocation pairs. Two access methods are defined: one for locating certificates issued to the certificate issuer and one for locating an OCSP server that provides status information about this certificate. Certificates issued under the Common Certificate Policy must include an authorityInfoAccess extension with at least one instances of the calssuers access method: that specifies an HTTP URI. The OCSP access method must also be included since the Common Policy mandates OCSP distribution of status information for this certificate.
AccessDescription			
accessMethod		id-ad-calssuers (1.3.6.1.5.5.7.48.2)	When this access method is used, the access location should use the URI name form to specify the location of an LDAP accessible directory server or HTTP accessible Web server where certificates issued to the issuer of this certificate may be found.
accessLocation			
GeneralName			
uniformResourceIdentifier		ldap://… or http://…	See preamble text on URIs.
accessMethod		id-ad-ocsp (1.3.6.1.5.5.7.48.1)	When this access method is used, the access location should use the URI name form to specify the location of an HTTP accessible OCSP server distributing status information for this certificate.
accessLocation			
GeneralName			
uniformResourceIdentifier		http://…	See preamble text on URIs.
subjectAltName	FALSE		
GeneralNames			This extension MUST include a UUID as specified below. Any additional name types may be present. Other names may be included to support local applications.
GeneralName			
uniformResourceIdentifier		urn:uuid:…	A UUID encoded as a URN, as specified in Section 3 of RFC 4122.
piv-interim (2.16.840.1.101.3.6.9.1)	FALSE		The PIV interim indicator extension is defined in appendix D.2 of FIPS 201-1.

Field	Criticality Flag	Value	**Comments**
interim_indicator		BOOLEAN	The value of this extension is asserted as follows: • TRUE if, at the time of credential issuance, (1) the FBI National Criminal History Fingerprint Check has completed successfully, and (2) a NACI has been initiated but has not completed. • FALSE if, at the time of credential issuance, the subject's NACI has been completed and successfully adjudicated.
optional extensions			
issuerAltName	FALSE		Any name types may be present; only the most common are specified here.
GeneralNames			
GeneralName			
rfc822Name		IA5String	Electronic mail address of the PKI administration
extKeyUsage	FALSE		This extension need not appear. If included to support specific applications, the extension may include the anyExtendedKeyUsage value. The 2 values listed are recommended for authentication purposes. Additional key purposes may be specified. Note: Organizations that choose not to include the *anyExtendedKeyUsage* value may experience interoperability issues if the specific EKU required by an application is absent.
		1.3.6.1.5.2.3.4	id-pkinit-KPClientAuth
		1.3.6.1.5.5.7.3.2	TLS client authentication
		2.5.29.37.0	anyExtendedKeyUsage OID indicates that the certificate may also be used for other purposes meeting the requirements specified in the key usage extension.
Designed by Robert Moskowitz (ICSA) and modified by Booz Allen & Hamilton and NIST			

Commented [MDK1]: The certificate profiles will be updated according to the EKU change Proposal as appropriate

Estimated Cost:

There is no cost to implement this change for CAs that do not issue certificates under the new policy OIDs.

Implementation Date:

This change will be effective upon approval by the FPKIPA and incorporation into the Federal Common Policy Framework Certificate Policy.

Prerequisites for Adoption:

Before certificates may be issued under the two new policy OIDs specified in this change proposal, [CCP-PROF] will be updated.

No Derived PIV credentials shall be issued unless the issuer has met the requirements of and is operating under the Guidelines of NIST SP 800-79 as exhibited by the subscribing agency's 800-79 ATO.

Plan to Meet Prerequisites:

Not Applicable

Approval and Coordination Dates:

Date presented to CPWG:	March 18, 2014
Date presented to FPKIPA:	April 7, 2015
Date of approval by FPKIPA:	April 15, 2015