Common Policy and Certificate Profiles Change Proposal Number: 2018-03

To:	Federal PKI Policy Authority (FPKIPA)
From:	FPKIMA
Subject:	Mandate specific EKU in Common Policy Certificate Profiles to align with Industry Practices
Date:	January 19, 2018

Title: Mandate specific EKU in Common Policy CP and its associated Certificate Profiles

X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework Version 1.28 April 4, 2018

X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program, July 17, 2017 [Common Profiles]

Change Advocate's Contact Information:
Name: Darlene Gore
Organization: FPKI Management Authority
Telephone number: 703-306-6109
E-mail address: darlene.gore@gsa.gov

Organization requesting change: FPKIMA

Change summary: Update the Certificate Profiles to mandate specific EKU and prohibit anyEKU

Background:

In 2015 the FPKIPA approved a change to the FPKI certificate profiles to make the Extended Key Usage (EKU) value of anyEKU optional when specific EKU values were asserted in end-entity certificates. At that time the community was not willing to prohibit the anyEKU value since they were not sure if there would be interoperability issues. It was proposed that the issue be revisited after seeing if there were issues with the certificates issued without the anyEKU value.

Some issuers within the FPKI community have been including only specific EKU in certificates since before 2015 with no interoperability issues and it is time to revisit the prohibition of anyEKU in light of the move toward creating different federal roots for different use cases for distribution in public trust stores.

This change proposal documents the requested change.

Specific Changes:

To Common Policy CP:

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

…

For End Entity certificates issued after June 30, 2019, the Extended Key Usage extension shall always be present and shall not contain *anyExtendedKeyUsage* {2.5.29.37.0}. Extended Key Usage OIDs shall be consistent with key usage bits asserted.

If a certificate is used for authentication of ephemeral keys, the Key Usage bit in the certificate must assert the DigitalSignature bit and may or may not assert Key Encryption and Key Agreement depending on the public key in the SPKI of the certificate.

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]).

Changes to certificate profile worksheets

Worksheet 5: End Entity Signature Certificate Profile: (in [Common Profiles])
Move these rows from optional extensions up to the mandatory extensions section with the following modifications:

extKeyUsage	BOOLEAN		This extension ~~need not~~ MUST ~~-~~ appear in certificates issued after June 30, 2019. ~~If included to support specific applications, the~~ The extension should be non-critical and ~~may~~ shall not include the anyExtendedKeyUsage value. ~~If anyExtendedKeyUsage is not included, the~~ The ~~3~~ values listed below for keyPurposeID are recommended for inclusion~~should be included for signing purposes~~. Additional ~~key purposesk~~eyPurposeIDs consistent with signature purposes may be specified. Note: For certificates issued prior to June 30, 2019, anyExtendedKeyUsage may be present or the entire extension may be absent.~~Organizations that choose not to include the anyExtendedKeyUsage value may experience interoperability issues if the specific EKU required by an application is absent.~~
KeyPurposeId		1.3.6.1.5.5.7.3.4	Id-kp-emailProtection
		1.3.6.1.4.1.311.10.3.12	MSFT Document Signing
		1.2.840.113583.1.1.5	Adobe Certified Document Signing Note: this value is optional as Adobe has deprecated its use
		~~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.~~

Worksheet 6: Key Management Certificate Profile: (in [Common Profiles])
Move these rows from optional extensions up to the mandatory extensions section with the following modifications:

extKeyUsage	BOOLEAN		This extension ~~need not~~ MUST appear in certificates issued after June 30, 2019. ~~If included to support specific applications, the~~ The extension should be non-critical and ~~may~~ shall not include the anyExtendedKeyUsage value. ~~If anyExtendedKeyUsage is not included, the~~ The ~~2~~ values listed below for keyPurposeID are recommended for inclusion.~~should be included for key management purposes~~. Additional ~~key purposes~~ keyPurposeIds consistent with key management purposes may be specified. Note: for certificates issued prior to TBD anyExtendedKeyUsage may be present or the entire extension may be absent.~~Organizations that choose not to include the anyExtendedKeyUsage value may experience interoperability issues if the specific EKU required by an application is absent.~~
KeyPurposeId		1.3.6.1.5.5.7.3.4	Id-kp-emailProtection
		~~1.3.6.1.4.1.311.10.3.4~~	~~Encrypting File System~~
		~~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.~~

Worksheet 9: PIV Authentication Certificate Profile: ([Common Profiles])
Move these rows from optional extensions up to the mandatory extensions section with the following modifications:

extKeyUsage	BOOLEAN		This extension ~~need not~~ MUST appear in end user certificates issued after June 30, 2019. ~~If included to support specific applications, the~~ The extension should be non-critical and ~~may~~ shall not include the anyExtendedKeyUsage value. ~~If anyExtendedKeyUsage is not included, the~~ The ~~3~~ values listed below for keyPurposeID are recommended for inclusion~~should be included for authentication purposes~~. Additional ~~key purposes~~ keyPurposeIds consistent with authentication purposes may be specified. Note: for certificates issued prior to June 30, 2019, anyExtendedKeyUsage may be present or the entire extension may be absent.~~Organizations that choose not to include the anyExtendedKeyUsage value may~~

			~~experience interoperability issues if the specific EKU required by an application is absent.~~
KeyPurposeId		1.3.6.1.4.1.311.20.2.2	Microsoft Smart card Logon
		1.3.6.1.5.5.7.3.2	TLS client authentication
		1.3.6.1.5.2.3.4	Id-pkinit-KPClientAuth
		1.3.6.1.5.5.7.3.21	Id-kp-secureShellClient Note: This key purpose value may be implemented as needed by the Subscriber, eg. may only be required for administrators
		~~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.~~

Worksheet 7: Certificate Profile for Computing and Communications Devices: ([Common Profiles])
Move these rows from optional extensions up to the mandatory extensions section with the following modifications:

keyUsage	TRUE		Use of a single certificate for both digital signatures and key management is deprecated, but may be used to support legacy applications that require the use of such certificates.
digitalSignature		1	May be asserted. Note: If a certificate is used for authentication of ephemeral keys, the Key Usage bit in the certificate must assert the DigitalSignature bit and may ~~or may not~~ assert Key Encryption and Key Agreement depending on the public key in the SPKI of the certificate only if required
...			
extKeyUsage	BOOLEAN		This extension ~~may~~MUST be included as either a critical or non-critical extension in certificates issued after June 30, 2019 ~~if its inclusion is required by the application(s) for which the certificate will be used.~~ Additional key purposes consistent with keyUsage may be specified. The extension may not include the anyExtendedKeyUsage value. Note: this extension may be absent in certificates issued prior to June30, 2019. There is a separate profile for PIV Content Signing Certificates – see Worksheet 10
~~KeyPurposeId~~		~~2.16.840.1.101.3.6.7~~	~~The id-PIV-content-signing keyPurposeID specifies that the public key may be used to verify signatures on PIV CHUIDs and PIV biometrics. No other EKU shall be~~

			~~included when id-PIV-content-signing is asserted.~~

Worksheet 10: Common PIV Content Signing Certificate Profile (in [Common Profiles]) (Note the addition was missed from the Devices profile when Worksheet 10 was created – this just corrects the typo)

KeyPurposeId		2.16.840.1.101.3.6.7	The id-PIV-content-signing keyPurposeID specifies that the public key may be used to verify signatures on PIV CHUIDs and PIV biometrics. No other EKU shall be included when id-PIV-content-signing is asserted.

Worksheet 11: Derived PIV Authentication Certificate Profile: ([Common Profiles])
Move these rows from optional extensions up to the mandatory extensions section with the following modifications:

extKeyUsage	BOOLEAN		This extension ~~need not~~ MUST appear in end user certificates issued after June 30, 2019. ~~If included to support specific applications, the~~ The extension should be non-critical and ~~may~~ shall not include the anyExtendedKeyUsage value. ~~If anyExtendedKeyUsage is not included, the~~ The ~~following~~ 2 values listed below for KeyPurposeId must be included. ~~id-pkinit-KPClientAuth and TLS client authentication.~~ Additional keyPurposeIds consistent with authentication purposes may be specified. Note: For certificates issued prior to June 30, 2019, anyExtendedKeyUsage may be present or the entire extension may be absent. ~~Organizations that choose not to include the anyExtendedKeyUsage value may experience interoperability issues if the specific EKU required by an application is absent.~~
KeyPurposeId		1.3.6.1.5.5.7.3.2	TLS client authentication
		1.3.6.1.5.2.3.4	Id-pkinit-KPClientAuth
		~~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.~~

Delta Mapping: Not applicable

Estimated Cost: The cost of complying with this change will depend on your PKI service provider and the number of certificate configurations that must be changed.

Implementation Date: June 30, 2019.

Prerequisites for Adoption: none

Plan to Meet Prerequisites: Not applicable

Approval and Coordination Dates:

Date presented to PA/CPWG:	1/19/2018
Date change released for comment:	1/19/2018
Date published:	May 8, 2018