



**FBCA Certificate Policy Change Proposal Number: 2018-03**

**Including Changes to Certificate Profiles.**

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

---

**Title:** Mandate specific EKU in the FBCA CP and its associated Certificate Profiles

- X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA) Version 2.32, 4 April 2018
- Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile, July 17, 2017, [FPKI Profiles]
- X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards, July 17, 2017 [PIV-I 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 not allow 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 FBCA 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 certificate.

PIV-I Content Signing certificates shall include an extended key usage of id-fpki-pivi-content-signing (see [PIV-I Profile]).

## Changes to certificate profile worksheets

Worksheet 5: End Entity Signature Certificate Profile: in [FPKI Profiles]

And

Worksheet 6: PIV-I Digital Signature Certificate Profile: in [PIV-I Profiles]

Move these rows from optional extensions up to the mandatory extensions section with the following modifications:

extKeyUsage	BOOLEAN		<del>This extension need not MUST-appear in certificates issued after June 30, 2019. If included to support specific applications, the</del> The extension should be non-critical and <del>may</del> shall not include the anyExtendedKeyUsage value. <del>If anyExtendedKeyUsage is not included, the</del> The 3-values listed below for keyPurposeID are recommended for inclusion <del>should be included for signing purposes.</del> Additional <del>key-purposes</del> keyPurposeIDs, consistent with signing purposes, may be specified. Note: For certificates issued prior to June 30, 2019, <del>anyExtendedKeyUsage may be present or the entire extension may be absent. Organizations that choose not to include the</del> 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 has been deprecated by Adobe
		<del>2.5.29.37.0</del>	<del>anyExtendedKeyUsage OID indicates that the certificate may also be used for other purposes meeting the requirements specified in the key</del>

			usage extension.
--	--	--	------------------

Worksheet 6: Key Management Certificate Profile: in [FPKI Profiles]

And

Worksheet 7: PIV-I Key Management Certificate Profile: in [PIV-I Profiles]

Move these rows from optional extensions up to the mandatory extensions section with the following modifications:

extKeyUsage	BOOLEAN		<del>This extension need not MUST-</del> <del>appear in certificates issued after</del> <del>June 30, 2019. If included to-</del> <del>support specific applications, the</del> <del>The</del> extension should be non- critical and <del>may shall not</del> include the anyExtendedKeyUsage value. <del>If</del> <del>anyExtendedKeyUsage is not-</del> <del>included, the The</del> 2 values listed <del>below for keyPurposeID are</del> <del>recommended for inclusion should-</del> <del>be included for key management</del> <del>purposes.</del> Additional key- <del>purposeskeyPurposelds, consistent</del> <del>with key management purposes,</del> may be specified. Note: <del>For certificates issued prior to</del> <del>June 30, 2019,</del> <del>anyExtendedKeyUsage may be</del> <del>present or the entire extension may</del> <del>be absent. Organizations that</del> <del>choose not to include the-</del> <del>anyExtendedKeyUsage value may</del> <del>experience interoperability issues if</del> <del>the specific EKU required by an</del> <del>application is absent.</del>
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	<del>anyExtendedKeyUsage OID-</del> <del>indicates that the certificate may-</del> <del>also be used for other purposes-</del> <del>meeting the requirements specified-</del> <del>in the key usage extension.</del>

Worksheet 5: PIV-I Authentication Certificate Profile: ([PIV-I Profiles])

Move these rows from optional extensions up to the mandatory extensions section with the following modifications:

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

			<del>choose not to include the anyExtendedKeyUsage value may experience interoperability issues if the specific EKU required by an application is absent.</del>
KeyPurposeld		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
		<del>2.5.29.37.0</del>	<del>anyExtendedKeyUsage OID indicates that the certificate may also be used for other purposes meeting the requirements specified in the key usage extension.</del>

**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 comment adjudication published:	2/21/2018
Date published:	5/8/2018