General Purpose Extended Key Usage (EKU) for Document Signing X.509 Certificates draft-ito-documentsigning-eku-01

Tadahiko Ito, Sean Turner, Tomofumi Okubo

July X, 2021

Background

- Extended Key Usage [RFC5280, 4.2.1.12.]
  - This extension indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension.

- Usage of an EKU is a common practice, but we do not have a public and general EKU explicitly assigned for Document Signing certificates.

Decimal	Description	References
1	id-kp-serverAuth	[RFC2459]
2	id-kp-clientAuth	[RFC2459]
3	id-kp-codeSigning	[RFC2459]
4	id-kp-emailProtection	[RFC2459]
5	id-kp-ipsecEndSystem	Reserved and Obsolete
6	id-kp-ipsecTunnel	Reserved and Obsolete
7	id-kp-ipsecUser	Reserved and Obsolete
8	id-kp-timeStamping	[RFC2459]
9	id-kp-OCSPSigning	[RFC2560]
10	id-kp-dvcs	[RFC3029]
11	id-kp-sbgpCertAAServerAuth	Reserved and Obsolete
12	id-kp-scvp-responder	Reserved and Obsolete
13	id-kp-eapOverPPP	[RFC4334]
14	id-kp-eapOverLAN	[RFC4334]
15	id-kp-scvpServer	[RFC5055]
16	id-kp-scvpClient	[RFC5055]
17	id-kp-ipsecIKE	[RFC4945]
18	id-kp-capwapAC	[RFC5415]
19	id-kp-capwapWTP	[RFC5415]
20	id-kp-sipDomain	[RFC5924]
21	id-kp-secureShellClient	[RFC6187]
22	id-kp-secureShellServer	[RFC6187]
23	id-kp-sendRouter	[RFC6494]
24	id-kp-sendProxiedRouter	[RFC6494]
25	id-kp-sendOwner	[RFC6494]
26	id-kp-sendProxiedOwner	[RFC6494]
27	id-kp-cmcCA	[RFC6402]
28	id-kp-cmcRA	[RFC6402]
29	id-kp-cmcArchive	[RFC6402]
30	id-kp-bgpsec-router	[BGPSEC]

[RFC7299]

Current Practice (which OID for EKU are we using for document sign?)

- Usage of id-kp-emailProtection or id-kp-codesigning
  - May cause unexpected behaviors or have an adverse impact such as decreased cryptographic agility on the document signing ecosystem and vice versa
- Vendor-defined EKUs used for document signing
  - Adobe, Microsoft, and some other vendors for their own document signing products.
  - There are no issues if the vendor defined OIDs are used in a PKI (or a trust program) governed by the vendor
  - If the OID is used outside of the vendor governance, the usage can easily become out of control

What would be other choices?

- OIDs for EKU could be individually defined by
  - Nation state, forums, consortiums, software vendors, individual CAs, etc.
- Those EKU might works as well,
  - IF, they are willing to spend resource to govern and manage the OID alongside with the governing policy (not all organizations may have a reasonably large scale document signing to do that)
- Issues
  - What happen if the user base is small scale, for instance, an application for enterprise internal use, or do not have resource to assign and manage the OID?
  - If the usage is cross-national, forums, CAs, etc., they might need to be careful with unexpected behaviors or have an adverse impact such as decreased cryptographic agility

Our proposal

- An EKU for General Document Signing
  - For certificates, that are intended to be used for signing contents that are consumed by humans.
  - "Contents" is something printable or displayable, rather than processed by machines.

- OID to be assigned by IANA
  - Dedicated for a document signing mechanism and can be used for any existing policies.
  - Allows id-kp-emailProtection, id-kp-codesigning etc. to be protected from cross-contamination due to unintended usage (e.g. certs only used for document signing).

- CAs can include multiple EKUs (e.g. policy specific EKU, id-kp-emailProtection, etc.) related to document signing if they choose to do so.

> [RFC5280, 4.2.1.12.]
> If the extension is present, then the certificate MUST only be used for one of the purposes indicated.
> If multiple purposes are indicated the application need not recognize all purposes indicated, as long as the intended purpose is present. Certificate using applications MAY require that the extended key usage extension be present and that a particular purpose be indicated
> in order for the certificate to be acceptable to that application.