General Purpose Extended Key Usage (EKU) for Document Signing X.509 Certificates

Abstract

RFC5280 specifies several extended key purpose identifiers (KeyPurposeIds) for X.509 certificates. This document defines a general purpose document signing KeyPurposeId for inclusion in the Extended Key Usage (EKU) extension of X.509 public key certificates. Document Signing applications may require that the EKU extension be present and that a document signing KeyPurposeId be indicated in order for the certificate to be acceptable to that Document Signing application.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-lamps-documentsigning-eku/.

Discussion of this document takes place on the Limited Additional Mechanisms for PKIX and SMIME (LAMPS) Working Group mailing list (mailto:spasm@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/spasm/. Subscribe at https://www.ietf.org/mailman/listinfo/spasm/.

Source for this draft and an issue tracker can be found at https://github.com/lamps-wg/documentsigning-eku.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six
months and may be updated, replaced, or obsoleted by other documents
at any time. It is inappropriate to use Internet-Drafts as reference
material or to cite them other than as "work in progress."

This Internet-Draft will expire on 23 February 2023.

Copyright Notice

Table of Contents

1. Introduction

[RFC5280] specifies several extended key purpose identifiers
(KeyPurposeIds) for X.509 certificates. In addition, several
KeyPurposeIds have been added under the IANA repository "SMI
Security for PKIX Extended Key Purpose" [RFC7299]. While usage of
the "anyExtendedKeyUsage" KeyPurposeId is bad practice for publicly
trusted certificates, there is no public and general KeyPurposeId
explicitly assigned for Document Signing. The current practice is to

use id-kp-emailProtection, id-kp-codeSigning or a vendor-defined
KeyPurposeId for general document signing purposes.

In circumstances where code signing and S/MIME certificates are also
used for document signing, technical or policy changes made to the
code signing and S/MIME ecosystem may cause unexpected behaviors or
have an adverse impact such as decreased cryptographic agility on
the document signing ecosystem and vice versa.

There is no issue if the vendor-defined KeyPurposeIds are used in a
PKI governed by the vendor or a set of specific group of vendors.
However, if the KeyPurposeId is used outside of vendor governance,
the usage can easily become out of control. For instance, when the
end user encounters certificates with vendor-defined KeyPurposeIds,
they might want to ask that vendor about use of the certificate.
However, if those certificates were not governed by the
KeyPurposeIds owner but by another vendor, the vender who own the
KeyPurposeIds may not able to control use, or even do not know about
the use. - If the issuance of the cert is not under the control of
the KeyPurposeIds owner, it is hard to estimate the impact of change
to made on the KeyPurposeId. Changes related to KeyPurposeIds
possibly make negative impacts that some group of people do not
tolerate, and it could become a migration agility issue.

Therefore, it is not favorable to use a vendor-defined KeyPurposeId
for signing a document that is not governed by the vendor.

This document defines an extended key purpose identifier for
Document Signing.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and
"OPTIONAL" in this document are to be interpreted as described in
BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all
capitals, as shown here.

3. Extended Key Purpose for Document Signing

This specification defines the KeyPurposeId id-kp-documentSigning.

As described in [RFC5280], "[i]f the [Extended Key Usage] extension
is present, then the certificate MUST only be used for one of the
purposes indicated." [RFC5280] also describes that "[i]f multiple
[key] purposes are indicated the application need not recognize all
purposes indicated, as long as the intended purpose is present."

Document Signing applications MAY require that the Extended Key
Usage extension be present and that the id-kp-documentSigning be

indicated in order for the certificate to be acceptable to that
Document Signing application.

The term "Document Signing" in this document refers to digitally
signing contents that are consumed by people. To be more precise,
contents are intended to be shown to a person with printable or
displayable form by means of services or software, rather than
processed by machines.

3.1. Including the Extended Key Purpose for Document Signing in Certificates

[RFC5280] specifies the EKU X.509 certificate extension for use on
the Internet. The extension indicates one or more purposes for which
the certified public key is valid. The EKU extension can be used in
conjunction with the key usage extension, which indicates the set of
basic cryptographic operations for which the certified key may be
used.

The EKU extension syntax is repeated here for convenience:

```
ExtKeyUsageSyntax  ::=  SEQUENCE SIZE (1..MAX) OF KeyPurposeId
KeyPurposeId  ::=  OBJECT IDENTIFIER
```

As described in [RFC5280], EKU extension may, at the option of the
certificate issuer, be either critical or non-critical.

This specification defines the KeyPurposeId id-kp-documentSigning.
Inclusion of this KeyPurposeId in a certificate indicates that the
public key encoded in the certificate has been certified to be used
for cryptographic operations on contents that are consumed by
people.

```
id-kp  OBJECT IDENTIFIER  ::=
    { iso(1) identified-organization(3) dod(6) internet(1)
      security(5) mechanisms(5) pkix(7) 3 }
id-kp-documentSigning  OBJECT IDENTIFIER  ::=  { id-kp TBD2 }
```

4. Using the Extended Key Purpose for Document Signing in a Certificate

The signed contents of Internet-Drafts are primarily intended to be
consumed by people. To be more precise, contents are intended to be
shown to a person in a printable or displayable form by means of
services or software, rather than processed by machines. The digital
signature on the contents is to indicate to the recipient of the
contents that the content has not changed since it was signed by the
identity indicated as the subject of the certificate. To validate
the digital signature which is signed on contents intended to be

consumed by people, implementations MAY perform the steps below
during certificate validation:

The following procedure is used to examine the KeyPurposeId(s)
included in the Extended Key Usage extension. Restrictions on
Extended Key Usage is derived and implemented from (or configured
with) the policy to which the implementation conforms.

  *If there are no restrictions set for the relying party and the
   relying party software, the certificate is acceptable.

  *If there are restrictions set for the relying party and relying
   party software, then process the KeyPurposeId(s) as described
   below.

   This procedure is intended to permit or prohibit presence of a
   certain KeyPurposeId or complete absence of KeyPurposeIds. It is
   outside the scope of this document, but the relying party can
   permit or prohibit combinations of KeyPurposeIds, instead of
   single KeyPurposeId. A consideration on prohibiting combinations
   of KeyPurposeIds is described in the Security Considerations
   section of this document. If both "Excluded KeyPurposeId" and
   "Permitted KeyPurposeId" exists, the relying party or the relying
   party software proresses each restriction on "Excluded
   KeyPurposeId" first, and then processes each restriction on
   "Permitted KeyPurposeId".

   Excluded KeyPurposeId procedure: "Excluded KeyPurposeId" is a
      KeyPurposeId which the relying party or the relying party
      software prohibits. Examples of "Excluded KeyPurposeId" are,
      presence of the anyExtendedKeyUsage KeyPurposeId or complete
      absence of the EKU extension in a certificate. If a
      KeyPurposeId of the certificate meets the conditions set by
      the "Excluded KeyPurposeId" restriction, the relying party or
      the relying party software rejects the certificate.

   Permitted KeyPurposeId procedure: "Permitted KeyPurposeId" is a
      KeyPurposeId which the relying party or the relying party
      software accepts. Examples of "Permitted KeyPurposeId" are,
      presence of this general document signing KeyPurposeId and/or
      protocol specific document signing-type KeyPurposeIds. If a
      KeyPurposeId of the certificate meets the condition set by a
      "Permitted KeyPurposeId" restriction, the certificate is
      acceptable. Otherwise, relying party or the relying party
      software rejects the certificate.

When a single application has the capability to process various data
formats, the software may choose to make the excluded and permitted

decisions separately in accordance with the format it is handling
(e.g. text, pdf, etc).

5. Implications for a Certification Authority

   The procedures and practices employed by a certification authority
   MUST ensure that the correct values for the EKU extension are
   inserted in each certificate that is issued. Unless certificates are
   governed by a vendor(s) specific PKI, certificates that indicate
   usage for document signing MAY include the id-kp-documentSigning
   KeyPurposeId. The inclusion of the id-kp-documentSigning
   KeyPurposeId does not preclude the inclusion of other KeyPurposeIds.

6. Security Considerations

   The usage of id-kp-documentSigning KeyPurposeId is to provide an
   alternative to id-kp-emailProtection being used for non-email
   purposes and id-kp-codeSigning being used to sign objects other than
   binary code. This extended key purpose does not introduce new
   security risks but instead reduces existing security risks by
   providing means to separate other extended key purposes used for
   communication protocols namely, TLS (id-kp-clientAuth) or S/MIME
   (id-kp-emailProtection) etc. in order to minimize the risk of cross-
   protocol attacks.

   To reduce the risk of specific cross-protocol attacks, the relying
   party or relying party software may additionally prohibit use of
   specific combinations of KeyPurposeIds.

   While a specific protocol or signing scheme may choose to come up
   with their own KeyPurposeIds, some may not have significant motive
   or resources to set up and manage their own KeyPurposeIds. This
   general document signing KeyPurposeId may be used as a stop-gap for
   those that intend to define their own KeyPurposeId or those who do
   not intend to set up a KeyPurposeId but still would like to
   distinguish document signing from other usages.

   Introduction of this id-kp-documentSigning KeyPurposeId does not
   introduce any new security or privacy concerns.

7. IANA Considerations

   IANA is requested to make one assignment for the TBD2 in the id-kp-
   documentSigning object identifier (OID), as defined in Section 3.1,
   in the "SMI Security for PKIX Extended Key Purpose"
   (1.3.6.1.5.5.7.3) registry. The other assignment for the TBD1 in
   Appendix A for the id-mod-docsign-eku ASN.1 module [X.680] object
   identifier (OID), as defined in Appendix A, in the "SMI Security for
   PKIX Module Identifier" (1.3.6.1.5.5.7.0) registry.

NOTE to the RFC Editor: After the assignment is made, the "for the
TBD*" phrase can be dropped prior to publication as an RFC.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
           Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/
           RFC2119, March 1997, <https://www.rfc-editor.org/rfc/
           rfc2119>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S.,
           Housley, R., and W. Polk, "Internet X.509 Public Key
           Infrastructure Certificate and Certificate Revocation
           List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May
           2008, <https://www.rfc-editor.org/rfc/rfc5280>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
           2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
           May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[X.680]   ITU-T, "Information technology - Abstract Syntax Notation
           One (ASN.1): Specification of basic notation", ISO/IEC
           8824-1:2015, November 2015.

8.2. Informative References

[RFC7299] Housley, R., "Object Identifier Registry for the PKIX
           Working Group", RFC 7299, DOI 10.17487/RFC7299, July
           2014, <https://www.rfc-editor.org/rfc/rfc7299>.

Appendix A. ASN.1 Module

The following ASN.1 module provides the complete definition of the
Document Signing KeyPurposeId.

```
DocSignEKU { iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) id-mod(0)
  id-mod-docsign-eku(TBD1) }

DEFINITIONS EXPLICIT TAGS ::=

BEGIN

-- EXPORTS ALL --

-- IMPORTS NOTHING --

-- OID Arc --

id-kp  OBJECT IDENTIFIER  ::= {
  iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) kp(3) }

-- Document Signing Extended Key Usage --

id-kp-documentSigning OBJECT IDENTIFIER ::= { id-kp TBD2 }

END
```

Acknowledgments

We would like to thank Russ Housley for verifying the ASN.1 module.
Additionally, we would like to thank Corey Bonnell, Wendy Brown,
Russ Housley, Prachi Jain, and Stefan Santesson for their comments.

Authors' Addresses

Tadahiko Ito
SECOM CO., LTD.

Email: tadahiko.ito.public@gmail.com

Tomofumi Okubo
DigiCert, Inc.

Email: tomofumi.okubo+ietf@gmail.com

Sean Turner
sn3rd

Email: sean@sn3rd.com