

Workgroup: LAMPS Working Group

Internet-Draft:

draft-ietf-lamps-documentsigning-eku-00

Published: 13 January 2022

Intended Status: Standards Track

Expires: 17 July 2022

Authors: T. Ito                      T. Okubo                      S. Turner

          SECOM CO., LTD.      DigiCert, Inc.      sn3rd

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

### **Abstract**

[[RFC5280](#)] specifies several extended key usages for X.509 certificates. This document defines a general purpose document signing extended key usage for X.509 public key certificates which restricts the usage of the certificates for document signing.

### **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/>.

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 17 July 2022.

## Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

- [1. Introduction](#)
- [2. Conventions and Definitions](#)
- [3. Extended Key usage for DocumentSigning](#)
  - [3.1. Extended Key Usage Values for Document Signing](#)
- [4. Using the Document Signing EKU in a Certificate](#)
- [5. Implications for a Certification Authority](#)
- [6. Security Considerations](#)
- [7. IANA Considerations](#)
- [8. Normative References](#)
- [Appendix A. ASN.1 Module](#)
- [Acknowledgments](#)
- [Authors' Addresses](#)

## 1. Introduction

[RFC5280] specifies several extended key usages for X.509 certificates. In addition, several extended key usage had been added[RFC7299] as public OID under the IANA repository. While usage of any extended key usage is bad practice for publicly trusted certificates, there are no public and general extended key usage explicitly assigned for Document Signing certificates. The current practice is to use id-kp-emailProtection, id-kp-codeSigning or vendor defined Object ID for general document signing purposes.

In circumstances where code signing and S/MIME certificates are also widely used for document signing, the technical or policy changes that are made to code signing and S/MIME certificates 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 OIDs are used in a PKI (or a trust program) governed by the vendor. However, if the OID is used

outside of the vendor governance, the usage can easily become out of control (e.g. - When the end user encounters vendor defined OIDs, they might want to ask that vendor about use of the certificate, however, the vendor may not know about the particular use. - If the issuance of the cert is not under the control of the OID owner, there is no way for the OID owner to know what the impact will be if any change is made to the OID in question, and it would restrict vendor's choice of OID management. etc.).

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

This document defines a general Document Signing extended key usage.

## **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 usage for DocumentSigning**

This specification defines the KeyPurposeId id-kp-documentSigning. Inclusion of this KeyPurposeId in a certificate indicates that the use of any Subject names in the certificate is restricted to use by a document signing.

Term of "Document Sign" in this document is digitally sign contents that are consumed by humans. To be more precise, contents are intended to be shown to human with printable or displayable form by means of services or software, rather than processed by machines.

### **3.1. Extended Key Usage Values for Document Signing**

[[RFC5280](#)] specifies the EKU X.509 certificate extension for use in 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 how the public key in the certificate is used, in a more basic cryptographic way.

The EKU extension syntax is repeated here for convenience:

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

This specification defines the KeyPurposeId id-kp-documentSigning. Inclusion of this KeyPurposeId in a certificate indicates that the

use of any Subject names in the certificate is restricted to use by a document signing service or a software (along with any usages allowed by other EKU values).

```
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 XX }
```

#### 4. Using the Document Signing EKU in a Certificate

[[RFC8358](#)] specifies the conventions for digital signatures on Internet-Drafts. This is one of the intended use cases for the general document signing EKU described in this document. [[RFC8358](#)] uses CMS to digitally sign a wide array of files such as ASCII, PDF, EPUB, HTML etc. Currently, there are no specification regarding EKU for certificates signing those files except those which are defined by the software vendor.

The signed contents of Internet-Drafts are primarily intended to be consumed by human. To be more precise, contents are intended to be shown to human in a printable or displayable form by means of services or software, rather than processed by machines. To validate the digital signature which is signed to contents intended to be consumed by human, implementations MAY perform the steps below as a certificate validation:

The implementation MAY examine the Extended Key Usage value(s):

1. If there are no restrictions set for the relying party and the relying party software, the certificate is acceptable.
2. If there are restrictions set for the replying party and relying party software, proceed as following.

Each Restriction on the EKUs can be "Excluded EKU" or "Permitted EKU" and handled.

The procedure is intended to permit or prohibit presence of a certain EKU or complete absence of EKUs. It is outside the scope of this document, but the relying party can permit or prohibit combinations of EKU. A consideration on prohibiting combination of EKUs is described in the security consideration section of this document.

2.1. Excluded EKUs procedure "Excluded EKU" is an EKU which the relying party or the relying party software prohibits. Examples of "Excluded EKU" are, presence of anyEKU or complete absence of EKU extension on a certificate. If an EKU of the certificate meets the

conditions set by the "Excluded ECU" restriction, the relying party or the relying party software rejects the certificate.

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

When a single software has 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 ECU extension are inserted in each certificate that is issued. Unless certificates are governed by a vendor specific PKI (or trust program), certificates that indicate usage for document signing MAY include the id-kp-documentSigning ECU extension. This does not encompass the mandatory usage of the id-kp-documentSigning ECU in conjunction with the vendor specific ECU. However, this does not restrict the CA from including multiple EKUs related to document signing.

## **6. Security Considerations**

The usage of id-kp-documentSigning ECU intends to prevent id-kp-emailProtection from being used for none-email purposes and id-kp-codeSigning used to sign objects other than binary codes. This ECU does not introduce new security risks but instead reduces existing security risks by providing means to separate other EKUs used for communication protocols namely, TLS or S/MIME 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 combination of EKUs.

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

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

## 7. IANA Considerations

This document requests that IANA make two assignments. One for the id-kp-documentSigning object identifier (OID), as defined in [Section 3.1](#), for the ECU from the "SMI Security for PKIX Extended Key Purpose" (1.3.6.1.5.5.7.3) registry. Another for the id-mod-docsign-eku, as defined in Appendix A, for the ASN.1 module [[X.680](#)] from the in the "SMI Security for PKIX Module Identifier" (1.3.6.1.5.5.7.0) registry. No further action is necessary by IANA.

## 8. 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>>.
- [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>>.
- [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>>.
- [RFC8358] Housley, R., "Update to Digital Signatures on Internet-Draft Documents", RFC 8358, DOI 10.17487/RFC8358, March 2018, <<https://www.rfc-editor.org/rfc/rfc8358>>.
- [X.680] ITU-T, "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation", ISO/IEC 8824-1:2015, November 2015.

## Appendix A. ASN.1 Module

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

```
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.

## Authors' Addresses

Tadahiko Ito  
SECOM CO., LTD.

Email: [tadahiko.ito.public@gmail.com](mailto:tadahiko.ito.public@gmail.com)

Tomofumi Okubo  
DigiCert, Inc.

Email: [tomofumi.okubo+ietf@gmail.com](mailto:tomofumi.okubo+ietf@gmail.com)

Sean Turner  
sn3rd

Email: [sean@sn3rd.com](mailto:sean@sn3rd.com)