Individual
Internet-Draft
Intended status: Informational
Expires: October 3, 2021

T. Ito
SECOM CO., LTD.
T. Okubo
DigiCert, Inc.

April 01, 2021

General Purpose Extended Key Usage (EKU) for Document Signing X.509 Certificates
draft-ito-documentsigning-eku-00

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.

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 October 3, 2021.

Copyright Notice

Table of Contents

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 paper is digitaly signing human readable data or data that is intended to be human readable by means of services and software.

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. 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 specific PKI (or trust program), certificates that indicate usage for document signing MAY include the id-kp-documentSigning EKU extension. This does not encompass the mandatory usage of the id-kp-documentSigning EKU in conjunction with the vendor specific EKU. However, this does not restrict the CA from including multiple EKUs related to document signing.

5. Security Considerations

The Use of id-kp-documentSigning EKU can prevents the usage of id-kp-emailProtection for none-email purposes and id-kp-codeSigning for signing objects other than binary codes. An id-kp-documentSigning EKU value does not introduce any new security or privacy concerns.

6. IANA Considerations

The id-kp-documentSigning purpose requires an object identifier (OID). The objects are defined in an arc delegated by IANA to Limited Additional Mechanisms for PKIX and SMIME (lamps). No further action is necessary by IANA.

7. 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/info/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/info/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/info/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/info/rfc8174>.

Authors' Addresses

Tadahiko Ito
SECOM CO., LTD.

Email: tadahiko.ito.public@gmail.com

Tomofumi Okubo
DigiCert, Inc.

Email: tomofumi.okubo+ietf@gmail.com