Workgroup: LAMPS WG
Internet-Draft: draft-reddy-lamps-jose-eku-02
Published: 17 April 2023
Intended Status: Standards Track
Expires: 19 October 2023
Authors: T. Reddy J. Ekman D. Migault
Nokia Nokia Ericsson

X.509 Certificate Extended Key Usage (EKU) for (JOSE) and CBOR Object Signing and Encryption (COSE)

Abstract

RFC 5280 specifies several extended key purpose identifiers (KeyPurposeIds) for X.509 certificates. This document defines JSON Web Signature (JWS), JSON Web Encryption (JWE), CBOR Object Web Signature (CWS) and CBOR Object Web Encryption (CWE) KeyPurposeIds inclusion in the Extended Key Usage (EKU) extension of X.509 public key certificates. An application processing JWS, JWE, CWS or CWE may require that the EKU extension be present and that a JWS, JWE, CWS or CWE KeyPurposeId be indicated in order for the certificate to be acceptable to validate the JWS or CWS signature or to encrypt a key in JWE or CWE.

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 19 October 2023.

Copyright Notice

Table of Contents

1. Introduction

[RFC5280] specifies several extended key purpose identifiers (KeyPurposeIds) for X.509 certificates. In addition, the IANA repository "SMI Security for PKIX Extended Key Purpose" [RFC7299] includes a number of KeyPurposeIds. While usage of the anyExtendedKeyUsage KeyPurposeId is bad practice - especially but not only for for publicly trusted certificates (multi-purpose or single-purpose) - there are no extended key purpose identifiers explicitly assigned for JSON Web Signature (JWS) [RFC7515] JSON Web Encryption (JWE) [RFC7516] or their CBOR Object Signing and Encryption (COSE) [RFC9052] counterparts defined as CBOR Object Web Signature (CWS) and CBOR Object Web Encryption (CWE).

JSON Web Signature (JWS) and CBOR Object Web Signature (CWS) represents content secured with digital signatures or Message Authentication Codes (MACs) using JSON-based [RFC7159] data structures and CBOR-based [RFC8949] data structures. The JWS and CWS cryptographic mechanisms provide integrity protection for an arbitrary sequence of octets.

JSON Web Encryption (JWE) and CBOR Object Web Encryption (CWE) represents encrypted content using JSON-based data structures and CBOR-based data structures. The JWE and CWE cryptographic mechanisms encrypt and provide integrity protection for an arbitrary sequence of

octets. The cryptographic algorithms and identifiers to be used with the JSON Web Signature (JWS) and JSON Web Encryption (JWE), CBOR Object Web Signature (CWS) and CBOR Object Web Encryption (CWE) are defined in [RFC7518] and [RFC9052].

Network Functions (NFs) as part of the service-based architecture within the 5G System [TS23.501]. The Operators of 5G systems make use of an internal PKI to generate X.509 PKI certificates for the NFs in a 5G system. The certificates are used for the following purposes:

- Client and Server certificates for NFs in 5GC Service Based Architecture (Section 6.1.3c of [TS33.310])
- Certificates for signing Client Credentials Assertion (CCA) tokens using JWS (Section 13.3.8.2 of [TS33.501])
- Certificates for encrypting JSON objects in HTTP messages between Security Edge Protection Proxies (SEPPs) using JWE (Section 13.2.4.4 of [TS33.501]) and Section 6.3.2 of [TS33.210])
- Certificates for signing the OAuth 2.0 access tokens for service authorization to grant temporary access to resources provided by NF producers using JWS (Section 13.4.1 of [TS33.501])

If the purpose of the issued certificates is not restricted, i.e., the type of operations for which a public key contained in the certificate can be used are not specified, those certificates could be used for another purpose than intended, violating the CA policies, and increasing the risk of cross-protocol attacks. Failure to ensure proper segregation of duties means that a NF who generates the public/private keys and applies for a certificate to the operator CA, could obtain a certificate which can be misused for tasks that this NF is not entitled to perform. For example, a NF service consumer could impersonate NF service producers using its certificate. Another example, if the purpose of the certificate is for the NF service consumer is to use it as a client certificate, the NF with this client certificate and corresponding private key must not be allowed to sign the CCA. When a NF service producer receives the signed CCA from the NF service consumer, the NF would accept the token even if CCA is signed with a certificate not issued for this purpose.

The KeyPurposeId id-kp-serverAuth (Section 4.2.1.12 of [RFC5280]) can be used to identify that the certificate is for a server (e.g., NF service producer), and the KeyPurposeId id-kp-clientAuth (Section 4.2.1.12 of [RFC5280]) can be used to identify that the certificate is for a client (e.g., NF service consumer). However, there is no KeyPurposeIds to identify whether the certificate can be used to generate JWS, JWE, CWS or CWE.

Vendor-defined KeyPurposeIds that are used in a PKI governed by the vendor or a group of vendors pose no interoperability concern. Appropriating, or misappropriating as the case may be, KeyPurposeIds for use outside of their originally intended vendor or group of vendors controlled environment can introduce problems, the impact of which is difficult to determine. Therefore, it is not favorable to use vendor-defined KeyPurposeIds for JWS, JWE, CWS and CWE in deployments that are not governed by the vendor.

This document defines extended key purpose identifiers for JWS, JWE, CWS and CWE.

2. Terminology

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.

CBOR Object Web Signature (CWS): Signing Object of a CBOR Object Signing and Encryption (COSE) defined in Section 4 of [RFC9052].

CBOR Object Web Encryption (CWE): Encryption Object of a CBOR Object Signing and Encryption (COSE) defined in Section 4 of [RFC9052].

3. Extended Key Purpose for JWS, JWE, CWS and CWE

This specification defines the KeyPurposeIds id-kp-json, id-kp-cbor. 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 notes that "[i]f multiple [key] purposes are indicated the application need not recognize all purposes indicated, as long as the intended purpose is present."

Applications processing JWS, JWE, CWS or CWE MAY require the CBOR format or the JSON format be specified by the EKU extention id-kp-cbor or id-kp-json. In addition, such application MUST require the keyUsage extension be set to nonRepudiation (also designated as contentCommitment) for the signature calculation and/or to keyEncipherment for encryption of the secret key.

4. Including the Extended KeyPurpose for JWS and JWE in Certificates

[RFC5280] specifies the EKU X.509 certificate extension for use on end entity certificates. 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], the EKU extension may, at the option of the certificate issuer, be either critical or non-critical. This specification defines the KeyPurposeIds id-kp-json and id-kp-cbor. Inclusion of KeyPurposeId id-kp-json in a certificate indicates that the public key encoded in the certificate has been certified to be used for validating the JWS or that the public key encoded in the certificate has been certified to be used for encrypting the Content Encryption Key (CEK) in JWE (for example, encrypt the CEK with the recipient's public key using the RSAES-OAEP algorithm to produce the JWE Encrypted Key). The distinction between JWS and JWE is performed via the KU that is set to nonRepudiation for JWS and dataEncipherment for JWE.

Similarly, inclusion of KeyPurposeId id-kp-cbor in a certificate indicates that the public key encoded in the certificate has been certified to be used for validating the CWS or that the public key encoded in the certificate has been certified to be used for encrypting the CEK in CWE. The distinction between CWS and CWE is performed via the KU that is set to nonRepudiation for CWS and dataEncipherment for CWE.

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

id-kp-json OBJECT IDENTIFIER ::= { id-kp TBD1 }
id-kp-cbor OBJECT IDENTIFIER ::= { id-kp TBD2 }
```

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 as well as the KU extension are inserted in each certificate that is issued. The inclusion of the id-kp-json, id-kp-cbor KeyPurposeIds does not preclude the inclusion of other KeyPurposeIds.

6. Security Considerations

The Security Considerations of [RFC5280] are applicable to this document. This extended key purpose does not introduce new security risks but instead reduces existing security risks by providing means to identify if the certificate is generated to process JWS or CWS signature or to encrypt the CEK in JWE or CWE.

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

specific combinations of KeyPurposeIds. The procedure of using Excluded KeyPurposeId and Permitted KeyPurposeId by an relying party to permit or prohibit combinations of KeyPurposeIds is defined in Section 4 of [RFC9336]. Examples of Excluded KeyPurposeId include the presence of the anyExtendedKeyUsage KeyPurposeId or the complete absence of the EKU extension in a certificate. Examples of Permitted KeyPurposeId include the presence of JWS, JWE, CWS or CWE KeyPurposeId.

7. Privacy Considerations

In some security protocols, such as TLS 1.2 [RFC5246], certificates are exchanged in the clear. In other security protocols, such as TLS 1.3 [RFC8446], the certificates are encrypted. The inclusion of EKU extension can help an observer determine the purpose of the certificate. In addition, If the certificate is issued by a public certification authority, the inclusion of EKU extension can help an attacker to monitor the Certificate Transparency logs [RFC9162] to identify the purpose of the certificate.

8. IANA Considerations

IANA is requested to register the following OIDs in the "SMI Security for PKIX Extended Key Purpose" registry (1.3.6.1.5.5.7.3). This OID is defined in Section 4.

Decimal	Description	References
TBD1	id-kp-json	This-RFC
TBD2	id-kp-cbor	This-RFC

Figure 1: Table 1

IANA is also requested to register the following ASN.1[X.680] module OID in the "SMI Security for PKIX Module Identifier" registry (1.3.6.1.5.5.7.0). This OID is defined in Appendix A.

Decimal	Description	References
TBD5	id-mod-jose-and-cose-eku	This-RFC

Figure 2: Table 2

9. Contributors

The following individuals have contributed to this document:

German Peinado
Nokia

Email: german.peinado@nokia.com

10. Acknowledgments

We would like to thank Corey Bonnell, Ilari Liusvaara, Carl Wallace and Russ Housley for their useful feedback.

11. References

11.1. 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/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>.

[RFC7159] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", RFC 7159, DOI 10.17487/RFC7159, March 2014, <https://www.rfc-editor.org/info/rfc7159>.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <https://www.rfc-editor.org/info/rfc7515>.

[RFC7516] Jones, M. and J. Hildebrand, "JSON Web Encryption (JWE)", RFC 7516, DOI 10.17487/RFC7516, May 2015, <https://www.rfc-editor.org/info/rfc7516>.

[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>.

[RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <https://www.rfc-editor.org/info/rfc8949>.

[RFC9052] Schaad, J., "CBOR Object Signing and Encryption (COSE): Structures and Process", STD 96, RFC 9052, DOI 10.17487/RFC9052, August 2022, <https://www.rfc-editor.org/info/rfc9052>.

11.2. Informative References

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/info/rfc5246>.

[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>.

[RFC7518] Jones, M., "JSON Web Algorithms (JWA)", RFC 7518, DOI 10.17487/RFC7518, May 2015, <https://www.rfc-editor.org/info/rfc7518>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC9162] Laurie, B., Messeri, E., and R. Stradling, "Certificate Transparency Version 2.0", RFC 9162, DOI 10.17487/RFC9162, December 2021, <https://www.rfc-editor.org/info/rfc9162>.

[RFC9336] Ito, T., Okubo, T., and S. Turner, "X.509 Certificate General-Purpose Extended Key Usage (EKU) for Document Signing", RFC 9336, DOI 10.17487/RFC9336, December 2022, <https://www.rfc-editor.org/info/rfc9336>.

[TS23.501] "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; System architecture for the 5G System (5GS); Stage 2 (Release 18), 3GPP TS 23.501 V18.0.0 Dec 2022,", <https://www.3gpp.org/ftp/Specs/archive/23_series/23.501/23501-i00.zip>.

[TS33.210] "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects;Network Domain Security (NDS); IP network layer security (Release 17), 3GPP TS 33.210 V17.1.0 Sept 2022,", <https://www.3gpp.org/ftp/Specs/archive/33_series/33.210/33210-h10.zip>.

[TS33.310] "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network

Domain Security (NDS); Authentication Framework (AF) (Release 17), 3GPP 33.310 V17.4.0, Sept 2022,", <https://www.3gpp.org/ftp/Specs/archive/33_series/33.310/33310-h40.zip>.

[TS33.501] "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system (Release 17), , 3GPP TS:33.501 V17.7.0, Sept 2022,", <https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-h70.zip>.

[X.680] "ITU-T, "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation", ITU-T Recommendation X.680, February 2021.", <https://www.itu.int/rec/T-REC-X.680>.

[X.690] "ITU-T, "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU-T Recommendation X.690, February 2021,", <https://www.itu.int/rec/T-REC-X.690>.

Appendix A. ASN.1 Module

The following module adheres to ASN.1 specifications [X.680] and [X.690].

```
<CODE BEGINS>

JOSE-EKU
  { iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) id-mod(0)
  id-mod-jose-eku(TBD4) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- OID Arc

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

-- Extended Key Usage Values

id-kp-json OBJECT IDENTIFIER ::= { id-kp TBD1 }
id-kp-cbor OBJECT IDENTIFIER ::= { id-kp TBD2 }

END


<CODE ENDS>
```

Authors' Addresses

Tirumaleswar Reddy
Nokia
India

Email: kondtir@gmail.com

Jani Ekman
Nokia
Finland

Email: jani.ekman@nokia.com

Daniel Migault
Ericsson
Canada

Email: daniel.migault@ericsson.com