Internet Engineering Task Force (IETF)
Request for Comments: 9509
Category: Standards Track
ISSN: 2070-1721

T. Reddy.K
J. Ekman
Nokia
D. Migault
Ericsson

March 2024

X.509 Certificate Extended Key Usage (EKU) for 5G Network Functions

Abstract

RFC 5280 specifies several extended key purpose identifiers (KeyPurposeIds) for X.509 certificates. This document defines encrypting JSON objects in HTTP messages, using JSON Web Tokens (JWTs), and signing the OAuth 2.0 access tokens KeyPurposeIds for inclusion in the Extended Key Usage (EKU) extension of X.509 v3 public key certificates used by Network Functions (NFs) for the 5G System.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9509.

Table of Contents

1. Introduction

The operators of 5G ("fifth generation") systems as defined by 3GPP make use of an internal PKI to generate X.509 PKI certificates for the Network Functions (NFs) (Section 6 of [TS23.501]) in a 5G System. The certificates are used for the following purposes:

* Client and Server certificates for NFs in 5G Core (5GC) Service Based Architecture (SBA) (see Section 6.1.3c of [TS33.310] and Section 6.7.2 of [TS29.500])

* Client Credentials Assertion (CCA) uses JSON Web Tokens (JWTs) [RFC7519] and is secured with digital signatures based on the JSON Web Signature (JWS) [RFC7515] (see Section 13.3.8.2 of [TS33.501], and Section 6.7.5 of [TS29.500]).

* Certificates for encrypting JSON objects in HTTP messages between Security Edge Protection Proxies (SEPPs) using JSON Web Encryption (JWE) [RFC7516] (see Section 13.2.4.4 of [TS33.501], Section 6.3.2 of [TS33.210], Section 6.7.4 of [TS29.500], and Section 5.3.2.1 of [TS29.573]).

* Certificates for signing the OAuth 2.0 access tokens for service authorization to grant temporary access to resources provided by NF producers using JWS (see Section 13.4.1 of [TS33.501] and Section 6.7.3 of [TS29.500]).

[RFC5280] specifies several key usage extensions, defined via KeyPurposeIds, for X.509 certificates. Key usage extensions added to a certificate are meant to express intent as to the purpose of the named usage, for humans and for complying libraries. In addition, the IANA registry "SMI Security for PKIX Extended Key Purpose" [RFC7299] contains additional KeyPurposeIds. The use of the anyExtendedKeyUsage KeyPurposeId, as defined in Section 4.2.1.12 of [RFC5280], is generally considered a poor practice. This is especially true for publicly trusted certificates, whether they are multi-purpose or single-purpose, within the context of 5G Systems and the 5GC Service Based Architecture.

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, increasing the risk of cross-protocol attacks. Failure to ensure proper segregation of duties means that a NF that generates the public/private keys and applies for a certificate to the operator certification authority could obtain a certificate that can be misused for tasks that this NF is not entitled to perform. For example, a NF service consumer could potentially impersonate NF service producers using its certificate. Additionally, in cases where the certificate's purpose is intended for use by the NF service consumer as a client certificate, it's essential to ensure that the NF with this client certificate and the corresponding private key are not allowed to sign the Client Credentials Assertion (CCA). When a NF service producer receives the signed CCA from the NF service consumer, the NF should only accept the token if the CCA is signed with a certificate that has been explicitly 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 are currently no KeyPurposeIds for the other usages of certificates in a 5G System. This document addresses the above problem by defining the EKU extension of X.509 public key certificates for signing the JWT Claims Set using JWS, encrypting JSON objects in HTTP messages using JWE, and signing the OAuth 2.0 access tokens using JWS.

Vendor-defined KeyPurposeIds used within a PKI governed by the vendor or a group of vendors typically do not pose interoperability concerns, as non-critical extensions can be safely ignored if unrecognized. However, using or misusing KeyPurposeIds outside of their intended vendor-controlled environment can lead to interoperability issues. Therefore, it is advisable not to rely on vendor-defined KeyPurposeIds. Instead, the specification defines standard KeyPurposeIds to ensure interoperability across various implementations.

Although the specification focuses on a 5G use case, the standard KeyPurposeIds defined in this document can be used in other deployments.

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.

3. Extended Key Purpose for Network Functions

This specification defines the KeyPurposeIds id-kp-jwt, id-kp-httpContentEncrypt, and id-kp-oauthAccessTokenSigning and uses these, respectively, for: signing the JWT Claims Set of CCA using JWS, encrypting JSON objects in HTTP messages between Security Edge Protection Proxies (SEPPs) using JWE, and signing the OAuth 2.0 access tokens for service authorization to grant temporary access to resources provided by NF producers using JWS. 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."

Network Functions that verify the signature of a CCA represented as a JWT, decrypt JSON objects in HTTP messages between Security Edge Protection Proxies (SEPPs) using JWE, or verify the signature of an OAuth 2.0 access tokens for service authorization to grant temporary access to resources provided by NF producers using JWS SHOULD require that corresponding KeyPurposeIds be specified by the EKU extension. If the certificate requester knows the certificate users are mandated to use these KeyPurposeIds, it MUST enforce their inclusion. Additionally, such a certificate requester MUST ensure that the KeyUsage extension be set to digitalSignature or nonRepudiation (also designated as contentCommitment) for signature calculation and/or to keyEncipherment for secret key encryption.

4. Including the Extended Key Purpose 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. The inclusion of KeyPurposeIds id-kp-jwt, id-kp-httpContentEncrypt, and id-kp-oauthAccessTokenSigning in a certificate indicates that the public key encoded in the certificate has been certified for use in the following:

1. Validating the JWS Signature in JWT. The distinction between JWS and JWE is determined by the Key Usage (KU) that is set to digitalSignature or nonRepudiation for JWS and keyEncipherment for JWE.

2. Encrypting JSON objects in HTTP messages (for example, encrypting the content-encryption key (CEK) with the recipient's public key using the RSAES-OAEP algorithm to produce the JWE Encrypted Key). KU is set to keyEncipherment.

3. Signing OAuth 2.0 access tokens. In this case, KU is set to digitalSignature or nonRepudiation.

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

id-kp-jwt OBJECT IDENTIFIER ::= { id-kp 37 }
id-kp-httpContentEncrypt OBJECT IDENTIFIER ::= { id-kp 38 }
id-kp-oauthAccessTokenSigning OBJECT IDENTIFIER ::= { id-kp 39 }
```

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-jwt, id-kp-httpContentEncrypt, and id-kp-oauthAccessTokenSigning 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 the means to identify if the certificate is generated to sign the JWT Claims Set, signing the OAuth 2.0 access tokens using JWS, or encrypting the CEK in JWE for encrypting JSON objects in HTTP messages.

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 for allowing or disallowing combinations of KeyPurposeIds using Excluded KeyPurposeId and Permitted KeyPurposeId, as carried out by a relying party, is defined in Section 4 of [RFC9336]. Examples of Excluded KeyPurposeIds include the presence of the anyExtendedKeyUsage KeyPurposeId or the complete absence of the EKU extension in a certificate. Examples of Permitted KeyPurposeIds include the presence of id-kp-jwt, id-kp-httpContentEncrypt, or id-kp-oauthAccessTokenSigning KeyPurposeIds.

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 the 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 an EKU extension can help an attacker to monitor the Certificate Transparency logs [RFC9162] to identify the purpose of the certificate.

8. IANA Considerations

IANA has registered the following OIDs in the "SMI Security for PKIX Extended Key Purpose" registry (1.3.6.1.5.5.7.3). These OIDs are defined in Section 4.

Decimal	Description	References
37	id-kp-jwt	RFC 9509
38	id-kp-httpContentEncrypt	RFC 9509
39	id-kp-oauthAccessTokenSigning	RFC 9509

Table 1

IANA has registered 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
108	id-mod-nf-eku	RFC 9509

Table 2

9. References

9.1. 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>.

[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>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015,

<https://www.rfc-editor.org/info/rfc7519>.

[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>.

[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>.

9.2. 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>.

[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] 3GPP, "System architecture for the 5G System (5GS)", Release 18.4.0, 3GPP TS 23.501, December 2023, <https://www.3gpp.org/ftp/Specs/archive/23_series/23.501/23501-i40.zip>.

[TS29.500] 3GPP, "5G System; Technical Realization of Service Based Architecture; Stage 3", Release 18.4.0, 3GPP TS 29.500, December 2023, <https://www.3gpp.org/ftp/Specs/archive/29_series/29.500/29500-i40.zip>.

[TS29.573] 3GPP, "5G System; Public Land Mobile Network (PLMN) Interconnection; Stage 3", Release 18.5.0, 3GPP TS 29.573, December 2023, <https://www.3gpp.org/ftp/Specs/archive/29_series/29.573/29573-i50.zip>.

[TS33.210] 3GPP, "Network Domain Security (NDS); IP network layer security", Release 17.1.0, 3GPP TS 33.210, September 2022, <https://www.3gpp.org/ftp/Specs/archive/33_series/33.210/33210-h10.zip>.

[TS33.310] 3GPP, "Network Domain Security (NDS); Authentication Framework (AF)", Release 18.2.0, 3GPP TS 33.310, December 2023, <https://www.3gpp.org/ftp/Specs/archive/33_series/33.310/33310-i20.zip>.

[TS33.501] 3GPP, "Security architecture and procedures for 5G system", Release 18.4.0, 3GPP TS 33.501, December 2023, <https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-i40.zip>.

Appendix A. ASN.1 Module

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

```
<CODE BEGINS>
NF-EKU
  { iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) id-mod(0)
  id-mod-nf-eku (108) }

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-jwt OBJECT IDENTIFIER ::= { id-kp 37 }
id-kp-httpContentEncrypt OBJECT IDENTIFIER ::= { id-kp 38 }
id-kp-oauthAccessTokenSigning OBJECT IDENTIFIER ::= { id-kp 39 }

END
<CODE ENDS>
```

Acknowledgments

We would like to thank Corey Bonnell, Ilari Liusvaara, Carl Wallace, and Russ Housley for their useful feedback. Thanks to Yoav Nir for the secdir review, Elwyn Davies for the genart review, and Benson Muite for the intdir review.

Thanks to Paul Wouters, Lars Eggert, and ric Vyncke for the IESG review.

Contributor

The following individual has contributed to this document:

German Peinado
Nokia
Email: german.peinado@nokia.com

Authors' Addresses

Tirumaleswar Reddy.K
Nokia
India
Email: kondtir@gmail.com

Jani Ekman
Nokia
Finland
Email: jani.ekman@nokia.com

Daniel Migault
Ericsson
Canada
Email: daniel.migault@ericsson.com