Stream: Internet Engineering Task Force (IETF)
RFC: 9809
Category: Standards Track
Published: June 2025
ISSN: 2070-1721
Authors: H. Brockhaus *Siemens*
D. Goltzsche *Siemens Mobility*

RFC 9809
X.509 Certificate Extended Key Usage (EKU) for Configuration, Updates, and Safety-Critical Communication

Abstract

RFC 5280 defines the Extended Key Usage (EKU) extension and specifies several extended key purpose identifiers (KeyPurposeIds) for use with that extension in X.509 certificates. This document defines KeyPurposeIds for general-purpose and trust anchor configuration files, for software and firmware update packages, and for safety-critical communication to be included in the EKU extension of X.509 v3 public key certificates.

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/rfc9809.

Copyright Notice

Table of Contents

1. Introduction

Key purpose identifiers (KeyPurposeIds) added to the certificate's EKU extension [RFC5280] are meant to express intent as to the purpose of the named usage, for humans and complying libraries. A full list of KeyPurposeIds is maintained in the IANA registry "SMI Security for PKIX Extended Key Purpose" [SMI-PKIX-PURPOSE]. The use of the anyExtendedKeyUsage KeyPurposeId, as defined in Section 4.2.1.12 of [RFC5280], is generally considered a poor practice.

This document defines KeyPurposeIds for certificates that are used for the following purposes, among others:

- Validating signatures of general-purpose software configuration files.

- Validating signatures of trust anchor configuration files.
- Validating signatures of software and firmware update packages.
- Authenticating communication endpoints authorized for safety-critical communication.

If the purpose of an issued certificate is not restricted (i.e., the operations of the public key contained in the certificate can be used in unintended ways), the risk of cross-application attacks is increased. Failure to ensure adequate segregation of duties means that an application or system that generates the public/private keys and applies for a certificate to the operator Certification Authority (CA) could obtain a certificate that can be misused for tasks that this application or system is not entitled to perform. For example, management of trust anchors is a particularly critical task. A device could potentially accept a trust anchor configuration file signed by a service that uses a certificate with no EKU or with the KeyPurposeIds id-kp-codeSigning (Section 4.2.1.12 of [RFC5280]) or id-kp-documentSigning [RFC9336]. A device should only accept trust anchor configuration files if the file is verified 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 TLS WWW server, and the KeyPurposeId id-kp-clientAuth (Section 4.2.1.12 of [RFC5280]) can be used to identify that the certificate is for a TLS WWW client. However, there are currently no KeyPurposeIds for usage with X.509 certificates for safety-critical communication.

This document addresses the above problems by defining KeyPurposeIds for the EKU extension of X.509 public key certificates. These certificates are used either for signing files (general-purpose configuration files, trust anchor configuration files, and software and firmware update packages) or for safety-critical communication.

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

The definitions of these KeyPurposeIds are intentionally broad to allow their use in different deployments even though they were initially motivated by industrial automation and rail automation (see Appendix B). The details for each deployment need to be described in the relevant technical standards and certificate policies.

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.

This document uses terms defined in [RFC5280]. X.509 certificate extensions are defined using ASN.1 [X.680] [X.690].

The term "safety-critical communication" refers to communication that could, under certain conditions, lead to a state in which human life, health, property, or the environment is endangered. For the definition of "safety", see [NIST.SP.800-160] and [ISO.IEC.IEEE_12207].

3. Extended Key Purpose for Configuration Files, Update Packages, and Safety-Critical Communication

This specification defines the following KeyPurposeIds:

- id-kp-configSigning: Used for signing general-purpose configuration files.
- id-kp-trustAnchorConfigSigning: Used for signing trust anchor configuration files.
- id-kp-updatePackageSigning: Used for signing software or firmware update packages.
- id-kp-safetyCommunication: Used for authenticating communication peers for safety-critical communication.

As described in Section 4.2.1.12 of [RFC5280], "[i]f the [extended key usage] extension is present, then the certificate **MUST** only be used for one of the purposes indicated", and "[i]f multiple [key] purposes are indicated the application need not recognize all purposes indicated, as long as the intended purpose is present".

None of the KeyPurposeIds specified in this document are intrinsically mutually exclusive. Instead, the acceptable combinations of those KeyPurposeIds with others specified in this document and with other KeyPurposeIds specified elsewhere are left to the technical standards of the respective application and the certificate policy of the respective PKI. For example, a technical standard may specify the following: "Different keys and certificates must be used for safety-critical communication and for trust anchor updates, and a relying party must ignore the KeyPurposeId id-kp-trustAnchorConfigSigning if id-kp-safetyCommunication is one of the specified key purposes in a certificate." For example, the certificate policy may specify the following: "The id-kp-safetyCommunication KeyPuposeId should not be included in an issued certificate together with the KeyPurposeId id-kp-trustAnchorConfigSigning." Technical standards and certificate policies of different applications may specify other rules. Further considerations on prohibiting combinations of KeyPurposeIds is described in Section 6.

Systems or applications that verify the signature of a general-purpose configuration file or trust anchor configuration file, the signature of a software or firmware update package, or the authentication of a communication peer for safety-critical communication **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 for signature verification, to keyEncipherment for public key encryption, and keyAgreement for key agreement.

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 (KU) 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-configSigning, id-kp-trustAnchorConfigSigning, id-kp-updatePackageSigning, and id-kp-safetyCommunication in a certificate indicates that the public key encoded in the certificate has been certified for the following usages:

- id-kp-configSigning

  A public key contained in a certificate containing the KeyPurposeId id-kp-configSigning may be used for verifying signatures of general-purpose configuration files of various formats (e.g., XML, YAML, or JSON). Configuration files are used to configure hardware or software.

- id-kp-trustAnchorConfigSigning

  A public key contained in a certificate containing the KeyPurposeId id-kp-trustAnchorConfigSigning may be used for verifying signatures of trust anchor configuration files of various formats (e.g., XML, YAML, or JSON). Trust anchor configuration files are used to add or remove trust anchors to the trust store of a device.

- id-kp-updatePackageSigning

  A public key contained in a certificate containing the KeyPurposeId id-kp-updatePackageSigning may be used for verifying signatures of software or firmware update packages. Update packages are used to install software (including bootloader, firmware, safety-related applications, and others) on systems.

- id-kp-safetyCommunication

  A public key contained in a certificate containing the KeyPurposeId id-kp-safetyCommunication may be used to authenticate a communication peer for safety-critical communication based on TLS or other protocols.

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

id-kp-configSigning             OBJECT IDENTIFIER ::= { id-kp 41 }
id-kp-trustAnchorConfigSigning  OBJECT IDENTIFIER ::= { id-kp 42 }
id-kp-updatePackageSigning      OBJECT IDENTIFIER ::= { id-kp 43 }
id-kp-safetyCommunication       OBJECT IDENTIFIER ::= { id-kp 44 }
```

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 and the KU extension are inserted in each certificate that is issued. The inclusion of the id-kp-configSigning, id-kp-trustAnchorConfigSigning, id-kp-updatePackageSigning, and id-kp-safetyCommunication KeyPurposeIds does not preclude the inclusion of other KeyPurposeIds.

6. Security Considerations

The security considerations of [RFC5280] are applicable to this document. These EKU key purposes do not introduce new security risks but instead reduce existing security risks by providing the means to identify if a certificate is generated to verify the signature of a general-purpose or trust anchor configuration file, the signature of a software or firmware update package, or the authentication of a communication peer for safety-critical communication.

To reduce the risk of specific cross-protocol attacks, the relying party 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]. The technical standards and certificate policies of the application should explicitly enumerate requirements for excluded or permitted KeyPurposeIds or their combinations. It is out of scope of this document to enumerate those, but an example of excluded KeyPurposeIds can be the presence of the anyExtendedKeyUsage KeyPurposeId. Examples of allowed KeyPurposeIds combinations can be the presence of id-kp-safetyCommunication together with id-kp-clientAuth or id-kp-serverAuth.

7. Privacy Considerations

In some protocols (e.g., TLS 1.2 [RFC5246]), certificates are exchanged in the clear. In other protocols (e.g., TLS 1.3 [RFC8446]), 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, which may reveal private information of the certificate subject.

8. IANA Considerations

IANA has registered the following ASN.1 [X.680] module OID in the "SMI Security for PKIX Module Identifier" registry [SMI-PKIX-MOD]. This OID is defined in Appendix A.

Decimal	Description	Reference
117	id-mod-config-update-sc-eku	RFC 9809

Table 1

IANA has also registered the following OIDs in the "SMI Security for PKIX Extended Key Purpose" registry [SMI-PKIX-PURPOSE]. These OIDs are defined in Section 4.

Decimal	Description	Reference
41	id-kp-configSigning	RFC 9809
42	id-kp-trustAnchorConfigSigning	RFC 9809
43	id-kp-updatePackageSigning	RFC 9809
44	id-kp-safetyCommunication	RFC 9809

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>.

[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.680-202102-I/en>.

[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.690-202102-I/en>.

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>.

[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>.

[RFC9509] Reddy.K, T., Ekman, J., and D. Migault, "X.509 Certificate Extended Key Usage (EKU) for 5G Network Functions", RFC 9509, DOI 10.17487/RFC9509, March 2024, <https://www.rfc-editor.org/info/rfc9509>.

[Directive-2016_797] European Parliament, Council of the European Union, "Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union", May 2020, <https://eur-lex.europa.eu/eli/dir/2016/797/2020-05-28>.

[ERJU] Europe's Rail Joint Undertaking, "Shared Cybersecurity Services Specification - SP-SEC-ServSpec - V1.0", February 2025, <https://rail-research.europa.eu/wp-content/uploads/2025/03/ERJU-SP-Cybersecurity-Specifications-V1.0.zip>.

[ERJU-web] Europe's Rail Joint Undertaking, "Europe's Rail Joint Undertaking - System Pillar", <https://rail-research.europa.eu/system_pillar/>.

[EU-CRA] European Commission, "Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)", November 2024, <https://eur-lex.europa.eu/eli/reg/2024/2847/oj>.

[EU-STRATEGY] European Commission, "The EU's Cybersecurity Strategy for the Digital Decade", December 2020, <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>.

[NIST.SP.800-160] Ross, R., Winstead, M., and M. McEvilley, "Engineering Trustworthy Secure Systems", NIST SP 800-160v1r1, DOI 10.6028/NIST.SP.800-160v1r1, November 2022, <https://doi.org/10.6028/NIST.SP.800-160v1r1>.

[ISO.IEC.IEEE_12207] ISO/IEC/IEEE, "Systems and software engineering - Software life cycle processes", ISO/IEC/IEEE 12207:2017, November 2017, <https://www.iso.org/standard/63712.html>.

[NIS2] European Commission, "Directive (EU) 2022/2555 of the European Parliament and of the Council", December 2024, <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>.

[IEC.62443-4-2] IEC, "Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components", IEC 62443-4-2:2019, February 2019, <https://webstore.iec.ch/publication/34421>.

[IEC.62443-3-3] IEC, "Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels", IEC 62443-3-3:2013, August 2013, <https://webstore.iec.ch/publication/7033>.

[CE-marking] European Commission, "CE marking", <https://single-market-economy.ec.europa.eu/single-market/ce-marking_en>.

[SMI-PKIX-PURPOSE] IANA, "SMI Security for PKIX Extended Key Purpose", <https://www.iana.org/assignments/smi-numbers>.

[SMI-PKIX-MOD] IANA, "SMI Security for PKIX Module Identifier", <https://www.iana.org/assignments/smi-numbers>.

Appendix A. ASN.1 Module

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

```
<CODE BEGINS>

Automation-EKU
  { iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) id-mod(0)
    id-mod-config-update-sc-eku (117) }

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-configSigning            OBJECT IDENTIFIER ::= { id-kp 41 }
id-kp-trustAnchorConfigSigning OBJECT IDENTIFIER ::= { id-kp 42 }
id-kp-updatePackageSigning     OBJECT IDENTIFIER ::= { id-kp 43 }
id-kp-safetyCommunication      OBJECT IDENTIFIER ::= { id-kp 44 }

END

<CODE ENDS>
```

Appendix B. Use Cases

These use cases are only for informational purposes.

Automation hardware and software products strive to become more safe and secure by fulfilling mandatory, generic system requirements related to cybersecurity, e.g., driven by federal offices like the European Union Cyber Resilience Act [EU-CRA] governed by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy. Automation products connected to the Internet and sold in the EU after 2027 must bear the so-called "CE marking" [CE-marking] to indicate that they comply with the EU-CRA. Such regulation was announced in the 2020 EU Cybersecurity Strategy [EU-STRATEGY] and complements other legislation in this area, like the directive on measures for a high common level of cybersecurity for network and information systems (NIS) across the European Union [NIS2].

The 2020 EU Cybersecurity Strategy [EU-STRATEGY] suggests implementing and extending international standards such as [IEC.62443-4-2] and [IEC.62443-3-3]. Automation hardware and software products of diverse vendors that are connected on automation networks and the Internet can be used to build common automation solutions. Standardized attributes would allow transparency of security properties and interoperability for vendors in the context of software and firmware updates, general-purpose configuration, trust anchor configuration, and safety-critical communication.

A concrete example for automation is a rail automation system. The Europe's Rail web page [ERJU-web] states:

> The System Pillar brings rail sector representatives under a single coordination body. To achieve this, the System Pillar will deliver a unified operational concept and a functional, safe and secure system architecture, with due consideration of cyber-security aspects, focused on the European railway network to which Directive 2016/797 applies (i.e. the heavy rail network) as well as associated specifications and/or standards.

See [Directive-2016_797]. For details about the System Pillar, see [ERJU].

Acknowledgments

We would like to thank the authors of [RFC9336] and [RFC9509] for their excellent template.

We also thank all reviewers of this document for their valuable feedback.

Contributors

Szofia Fazekas-Zisch
Siemens AG
Breslauer Str. 5
90766 Fuerth
Germany
Email: szofia.fazekas-zisch@siemens.com
URI: https://www.siemens.com

Baptiste Fouques
Alstom
Email: baptiste.fouques@alstomgroup.com

Daniel Gutierrez Orta
CAF Signalling
Email: daniel.gutierrez@cafsignalling.com

Martin Weller
Hitachi Rail
Email: martin.weller@urbanandmainlines.com

Nicolas Poyet
SNCF
Email: nicolas.poyet@sncf.fr

Authors' Addresses

Hendrik Brockhaus
Siemens
Werner-von-Siemens-Strasse 1
80333 Munich
Germany
Email: hendrik.brockhaus@siemens.com
URI: https://www.siemens.com

David Goltzsche
Siemens Mobility
Ackerstrasse 22
38126 Braunschweig
Germany
Email: david.goltzsche@siemens.com
URI: https://www.mobility.siemens.com