LAMPS Working Group
Internet-Draft
Intended status: Standards Track
Expires: 18 August 2025

H. Brockhaus
Siemens
D. Goltzsche
Siemens Mobility
14 February 2025

X.509 Certificate Extended Key Usage (EKU) for Industrial Automation

draft-ietf-lamps-automation-keyusages-05

Commenté [MB1]: To better scope what automation we are talking about.

Abstract

RFC 5280 defines the Extended Key Usage (EKU) ~~ExtendedKeyUsage~~ extension and several extended key purposes ~~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 ~~Extended Key Usage (~~EKU~~)~~ extension of X.509 v3 public key certificates used by industrial automation and the Europe's Rail Joint Undertaking (ERJU) System Pillar.

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 18 August 2025.

Copyright Notice

Table of Contents

1. Introduction

Automation hardware and software products will strategically be more safe and secure by fulfilling mandatory, generic system requirements related to cyber security 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~~ Internet would bear the ~~so called~~so-called CE marking [CE-marking] to indicate that they comply. Such regulation was announced in the 2020 EU Cybersecurity Strategy [EU-STRATEGY], and complements other legislation in this area, specifically the NIS2 Framework, Directive on measures for a high common level of cybersecurity across the Union [NIS2]. 2020 EU Cybersecurity Strategy suggests to implement and extend international standards such as the Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components [IEC.62443-4-2] (IACS refers to industrial automation and control system) and the Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels [IEC.62443-3-3]. Automation hardware and software products of diverse vendors that are connected on automation networks and the I~~i~~nternet build common automation solutions. Harmonized attributes ~~would allow~~ facilitates transparency of security properties and interoperability for vendors in context of secure software and firmware updates, general-purpose configuration, trust anchor configuration, and secure safety communication.

An ~~concrete~~ example for ~~Automation~~ automation is a Rail Automation system. The Europe's Rail Joint Undertaking System Pillar [ERJU] will deliver a unified operational concept and a functional, safe, and secure system architecture with system requirements for Rail Automation. The deliverables include due consideration of cyber security aspects based on the IEC 62443 series of standards, focused on the European railway network to which Directive 2016/797 - Interoperability of the rail system within the EU [Directive-2016_797] applies.

Commenté [MB2]: Not sure what does that means. Also, not sure we need to make such claims in an RFC.

a mis en forme : Surlignage

a mis en forme : Surlignage

a mis en forme : Surlignage

Commenté [MB3]: That is?

a mis en forme : Surlignage

a mis en forme : Surlignage

a mis en forme : Surlignage

Commenté [MB4]: ?

Commenté [MB5]: What is meant here?

Commenté [MB6]: That is? Can we define the term?

Commenté [MB7]: Won't age well

Commenté [MB8]: This is good for initial draft version, but I don't think this OK for an RFC

The ERJU System Pillar Cyber Security Working Group makes use of PKIs to generate X.509 ~~PKI~~ certificates. The certificates 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.

Section ~~—~~4.2.1.12 of [RFC5280] specifies several extended key usages, defined via KeyPurposeIds, for X.509 certificates. KeyPurposeIds added to a certificate are meant to express intent as to the purpose of the named usage, for humans and for complying libraries. KeyPurposeIds are maintained in ~~In addition,~~ the IANA registry "SMI Security for PKIX Extended Key Purpose" [RFC7299] ~~contains additional KeyPurposeIds~~.

The use of the KeyPurposeId anyExtendedKeyUsage ~~KeyPurposeId~~, as defined in Section 4.2.1.12 of [RFC5280], is generally considered a poor practice. This is especially true for certificates, whether they are multi-purpose or single-purpose, within the context of ERJU System Pillar.

If the purpose of the issued certificates is not restricted (~~,~~ i.e., the type of operations for which a public key contained in ~~the~~a certificate can be used in unintended ways), increasing the risk of cross-application attacks. Failure to ensure ~~proper~~ adequate segregation of duties means that an application or system that generates the public/private keys and applies for a certificate to the operator Ccertification ~~authority~~ 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~~ a device could potentially accept a trust anchor configuration file signed by a service that uses a certificate with no EKU or with the KeyPurposeId 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 either used for signing files (general-purpose

Commenté [MB9]: Do we have a pointer to cite here?

Commenté [MB10]: To fix

Commenté [MB11]: Simplify

Commenté [MB12]: Can we add a short definition to the terminology?

configuration and trust anchor configuration files, software and firmware update packages) or are used for safety-critical communication.

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 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, the specification defines standard KeyPurposeIds to ensure interoperability across various vendors and industries.

Although the specification focuses on use in industrial automation, the definitions are intentionally broad to allow the use of the KeyPurposeIds defined in this document in other deployments as well. The context in which the KeyPurposeIds defined in this document are used is out of scope for this document. In other words, details must be described in technical standards and certificate policies for those implementations.

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 X.509 extensions are defined using ASN.1 [X.680] and [X.690].

3. Extended Key Purpose for Industrial Automation

This specification defines the KeyPurposeIds id-kp-configSigning, id-kp-trustAnchorConfigSigning, id-kp-updatePackageSigning, and id-kp-safetyCommunication. These key purposes are ~~and uses used~~ these, respectively, for: signing general-purpose configuration files or trust anchor configuration files, signing software or firmware update packages, or 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

a mis en forme : Surlignage

Commenté [MB13]: This section has nothing specific to automation. Also, the text above says the context where this is deployed is out of scope

Commenté [MB14]: Split the long sentence

Commenté [MB15]: Do we really need to reproduce this here?

certificate policy of the respective PKI. For example, a technical standard may specify: 'Different keys and certificates MUST be used for safety 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.' The certificate policy, for example, may specify: 'The KeyPuposeId 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~~are described in ~~the Security Considerations section of this document~~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 (for example, XML, YAML, or JSON). Configuration files are used to configure hardware or software.

Commenté [MB16]: I don't think this brings much.

Commenté [MB17]: Can we simply? There are several occurrences in the doc.

a mis en forme : Surlignage

Commenté [MB18]: Is?

* 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 (~~for example~~ for example, 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 secure 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~~CA 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-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 extended key usage key purposes do not introduce new security risks but instead reduce existing security risks by providing the means to identify if ~~the~~ 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~~ a relying party or ~~the~~ relying party software may additionally prohibit use of specific combinations of KeyPurposeIds. The procedure for allowing

Commenté [MB19]: Is?

Commenté [MB20]: Is?

Commenté [MB21]: Is this needed?

Commenté [MB22]: Is?

Commenté [MB23]: Add a reference

Commenté [MB24]: This is too generic, IMO

I know this was used in other similar docs, e.g., RFC9509

a mis en forme : Surlignage

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 specify concrete requirements for excluded or permitted KeyPurposeIds or their combinations. 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-clinetAuth or id-kp-serverAuth.

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~~CA, 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 is 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
TBD1	id-mod-automation-eku	This-RFC

Commenté [MB25]: This does not match the id-mod-eu-automation-eku used in the «ASN.1 Module"

Table 1

IANA is also requested to register 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
41	id-kp-configSigning	This-RFC
42	id-kp-trustAnchorConfigSigning	This-RFC
43	id-kp-updatePackageSigning	This-RFC
44	id-kp-safetyCommunication	This-RFC

Table 2

9. 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.

10. References

10.1. 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/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>.

[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>.

[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>.

10.2. 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/rfc/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/rfc/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/rfc/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/rfc/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/rfc/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/rfc/rfc9509>.

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

[ERJU] Europe's Rail Joint Undertaking, "SP-Cybersecurity-SharedCybersecurityServices - Review 3 Final Draft Specs (V0.90)", September 2024, <https://rail-research.europa.eu/wp-content/uploads/2023/10/ERJU_SP_CyberSecurity_Review3_Files.zip>.

[EU-CRA] European Commission, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020", September 2022, <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act>.

[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>.

[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", n.d., <https://single-market-economy.ec.europa.eu/single-market/ce-marking_en>.

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-eu-automation-eku (TBD1) }

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>
```

Commenté [MB26]: Distinct from the one in the IANA section

Appendix B. History of Changes

[RFC Editor: Please remove this appendix in the release version of the document.]

Changes from 04 -> 05:

* Addressed SECDIR review comments from Carl Wallace

Changes from 03 -> 04:

* Addressed Deb's AD review comments (see "AD Comments on draft-ietf-lamps-automation-keyusages")

* Added early allocated OIDs

Changes from 02 -> 03:

* Rename id-kp-trustanchorSigning to id-kp-trustAnchorConfigSigning

* Rename id-kp-updateSigning to id-kp-updatePackageSigning

* Fixed some nits

Changes from 01 -> 02:

* Updates Sections 3 and 6 addressing last call comments (see "WG Last Call for draft-ietf-lamps-automation-keyusages-01")

Changes from 01 -> 02:

* Implemented the changes requested during WGLC

Changes from 00 -> 01:

* Fixed some minor nids and wording issues

draft-ietf-lamps-automation-keyusages version 00:

* Updated document and filename after WG adoption

Changes from 00 -> 01:

* Updated last paragraph of Section 1 addressing WG adoption comments by Rich and Russ

* Updated name and OID of ASN.1 module

draft-brockhaus-lamps-automation-keyusages version 00:

* Broadened the scope to general automation use case and use ERJU as an example.

* Fixed some nits reported.

draft-brockhaus-lamps-eu-rail-keyusages version 00:

* Initial version of the document following best practices from RFC 9336 and RFC 9509

Contributors

Szofia Fazekas-Zisch
Siemens AG Digital Industries Factory Automation
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