



**SLOVENSKI STANDARD**  
**oSIST prEN 304 624 V1.0.0:2026**

**01-oktober-2026**

---

**Kibernetska varnost (CYBER) - CRA - Zahteve za kibernetsko varnost za infrastrukturo javnih ključev in programsko opremo za izdajanje digitalnih potrdil**

Cyber Security (CYBER) - CRA - Cybersecurity requirements for Public key infrastructure and digital certificate issuance software

**Sample Document**

**Ta slovenski standard je istoveten z: ETSI EN 304 624 V1.0.0 (2026-08)**

---

**ICS:**

35.030

Informacijska varnost

IT Security

**oSIST prEN 304 624 V1.0.0:2026**

**en**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

# Sample Document

get full document from [standards.iteh.ai](https://standards.iteh.ai)

# Draft ETSI EN 304 624 V1.0.0 (2026-08)



**Cyber security (CYBER);  
CRA;  
Cybersecurity requirements for public key infrastructure and  
digital certificate issuance software**

get full document from [standards.iteh.ai](https://standards.iteh.ai)

---

**Reference**DEN/CYBER-EUS-0015

---

---

**Keywords**certificate, CRA, cybersecurity, public key  
infrastructure

---

**ETSI**650 Route des Lucioles  
F-06921 Sophia Antipolis Cedex - FRANCE

---

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° w061004871

---

**Important notice**

The present document can be downloaded from the  
[ETSI Search & Browse Standards](#) application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed,  
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to  
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our  
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

---

**Notice of disclaimer & limitation of liability**

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.  
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

---

**Copyright Notification**

No part of this document may be reproduced in any form, by any means and in any media, without the prior written authorization of ETSI and except as expressly permitted below.

By way of exception and when the document is a normative deliverable (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)), ETSI authorizes to reproduce and incorporate into products, services and technical documentation only those extracts (e.g. templates) that are strictly necessary for the technical implementation of the normative deliverable, to ensure compliance with the latter. Nothing in this notice shall be construed as limiting any mandatory exceptions to copyright provided by applicable law.

© ETSI 2026.  
All rights reserved.

# Contents

|                                                             |    |
|-------------------------------------------------------------|----|
| Introduction .....                                          | 8  |
| 1 Scope .....                                               | 9  |
| 2 References .....                                          | 9  |
| 2.1 Normative references .....                              | 9  |
| 2.2 Informative references .....                            | 9  |
| 3 Definition of terms, symbols and abbreviations .....      | 11 |
| 3.1 Terms .....                                             | 11 |
| 3.2 Symbols .....                                           | 12 |
| 3.3 Abbreviations .....                                     | 12 |
| 4 Product context .....                                     | 13 |
| 4.0 Introduction .....                                      | 13 |
| 4.1 Product Functions .....                                 | 14 |
| 4.2 Product Architecture .....                              | 15 |
| 4.3 Operational Environment .....                           | 17 |
| 4.3.1 General description .....                             | 17 |
| 4.3.2 Physical/Hardware environment .....                   | 17 |
| 4.3.3 Logical/Software environment .....                    | 17 |
| 4.3.4 Connectivity aspects .....                            | 17 |
| 4.4 Distribution of Security Functions .....                | 18 |
| 4.5 Users .....                                             | 18 |
| 4.6 Use cases .....                                         | 18 |
| 4.6.1 Private PKI for non critical sectors (UC1) .....      | 19 |
| 4.6.2 Private PKI for critical entities (UC2) .....         | 19 |
| 4.6.3 Public PKI for critical entities (UC3) .....          | 19 |
| 4.6.4 Public basic PKI for critical entities (UC4) .....    | 20 |
| 4.6.5 Multi-authority PKI for critical entities (UC5) ..... | 20 |
| 5 Technical requirements for the products .....             | 20 |
| 5.1 Introduction - Applicability of the requirements .....  | 20 |
| 5.2 No known exploitable vulnerabilities .....              | 21 |
| 5.3 Secure by default configuration .....                   | 21 |
| 5.3.1 SDBC- Access control .....                            | 21 |
| 5.3.2 SBDC- Monitoring .....                                | 21 |
| 5.3.3 SBDC- Cryptography .....                              | 21 |
| 5.3.4 SBDC- Certificates .....                              | 22 |
| 5.4 Secure updates .....                                    | 22 |
| 5.5 Authentication and access control .....                 | 22 |
| 5.6 Confidentiality .....                                   | 23 |
| 5.6.1 CON - General .....                                   | 23 |
| 5.6.2 CON - Secure storage and communications .....         | 25 |
| 5.6.3 CON - Key management .....                            | 25 |
| 5.7 Integrity .....                                         | 25 |
| 5.7.1 INT - Monitoring .....                                | 25 |
| 5.7.2 INT - Certificate signing .....                       | 27 |
| 5.7.3 INT- CRL signing .....                                | 27 |
| 5.8 Data minimisation .....                                 | 27 |
| 5.8.1 DM - General .....                                    | 28 |
| 5.8.2 DM - Secret management .....                          | 28 |
| 5.9 Availability protection .....                           | 28 |
| 5.9.1 AP - Certificate suspension and revocation .....      | 28 |
| 5.9.2 AP - Certificate status services .....                | 29 |
| 5.9.3 AP - Key management .....                             | 30 |
| 5.10 Impact minimisation .....                              | 30 |
| 5.11 Minimisation of attack surfaces .....                  | 30 |
| 5.12 Exploitation mitigation mechanisms .....               | 31 |
| 5.12.1 EMM - Certificate issuance .....                     | 31 |

|        |                                                                      |    |
|--------|----------------------------------------------------------------------|----|
| 5.12.2 | EMM - Certificate status.....                                        | 33 |
| 5.12.3 | EMM - Certificate re-key .....                                       | 34 |
| 5.12.4 | EMM - Certificate modification .....                                 | 34 |
| 5.13   | Logging and monitoring.....                                          | 34 |
| 5.14   | Data removal and transparency .....                                  | 35 |
| 5.14.1 | DRT - Secret management.....                                         | 36 |
| 6      | Assessment criteria for compliance with technical requirements ..... | 36 |
| 6.1    | Introduction to the assessment and compliance criteria .....         | 36 |
| 6.2    | No known exploitable vulnerabilities.....                            | 38 |
| 6.3    | Secure by default configuration.....                                 | 39 |
| 6.3.1  | SBDC - Access control .....                                          | 39 |
| 6.3.2  | SBDC - Monitoring .....                                              | 40 |
| 6.3.3  | SBDC - Cryptography .....                                            | 41 |
| 6.3.4  | SBDC - Certificates .....                                            | 42 |
| 6.4    | Secure updates.....                                                  | 43 |
| 6.5    | Authentication and access control .....                              | 45 |
| 6.5.1  | AC - General.....                                                    | 45 |
| 6.6    | Confidentiality.....                                                 | 46 |
| 6.6.1  | CON - General.....                                                   | 47 |
| 6.6.2  | CON - Secure storage and communications .....                        | 50 |
| 6.6.3  | CON - Key management.....                                            | 51 |
| 6.7    | Integrity.....                                                       | 53 |
| 6.7.1  | INT - Monitoring .....                                               | 53 |
| 6.7.2  | INT - Certificate signing.....                                       | 56 |
| 6.7.3  | INT- CRL signing.....                                                | 57 |
| 6.8    | Data minimisation .....                                              | 58 |
| 6.8.1  | General.....                                                         | 58 |
| 6.8.2  | DM - Secret management .....                                         | 61 |
| 6.9    | Availability protection.....                                         | 62 |
| 6.9.1  | AP - Certificate suspension and revocation .....                     | 62 |
| 6.9.2  | AP - Certificate status services .....                               | 65 |
| 6.9.3  | AP - Key management.....                                             | 67 |
| 6.10   | Impact minimisation.....                                             | 68 |
| 6.11   | Minimisation of attack surfaces.....                                 | 69 |
| 6.12   | Exploitation mitigation mechanisms .....                             | 70 |
| 6.12.1 | EMM - Certificate issuance .....                                     | 70 |
| 6.12.2 | EMM - Certificate status.....                                        | 75 |
| 6.12.3 | EMM - Certificate re-key .....                                       | 78 |
| 6.12.4 | EMM - Certificate modification .....                                 | 78 |
| 6.13   | Logging and monitoring.....                                          | 79 |
| 6.14   | Data removal and transparency .....                                  | 83 |

|                               |                                                                                                                                       |           |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>Annex A (informative):</b> | <b>Relationship between the present document and the requirements of EU Regulation (EU) 2024/2847 – the Cyber Resilience Act.....</b> | <b>86</b> |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-----------|

|                               |                                                            |           |
|-------------------------------|------------------------------------------------------------|-----------|
| <b>Annex B (informative):</b> | <b>Security analysis.....</b>                              | <b>89</b> |
| B.1                           | Risk calculation.....                                      | 89        |
| B.2                           | Risk Assessment.....                                       | 90        |
| B.2.1                         | Likelihood risk factors.....                               | 90        |
| B.2.1.1                       | Deployment.....                                            | 90        |
| B.2.1.2                       | Network and Physical security .....                        | 91        |
| B.2.1.3                       | User expertise.....                                        | 91        |
| B.2.1.4                       | Interface exposure .....                                   | 91        |
| B.2.2                         | Impact risk factors .....                                  | 91        |
| B.3                           | Evaluate Risks .....                                       | 91        |
| B.4                           | Requirements applicability - threats mapping rational..... | 100       |

|                                  |            |
|----------------------------------|------------|
| <b>Annexes C to J: Void.....</b> | <b>110</b> |
|----------------------------------|------------|

|                             |                                                               |            |
|-----------------------------|---------------------------------------------------------------|------------|
| <b>Annex K (normative):</b> | <b>Generic cryptographic requirements and assessment.....</b> | <b>111</b> |
|-----------------------------|---------------------------------------------------------------|------------|

|     |                   |     |
|-----|-------------------|-----|
| K.1 | Cryptography..... | 111 |
|-----|-------------------|-----|

|                                                              |                                                                     |            |
|--------------------------------------------------------------|---------------------------------------------------------------------|------------|
| K.1.1                                                        | Requirement .....                                                   | 111        |
| K.1.2                                                        | Assessment of product cryptographic configuration .....             | 112        |
| K.1.2.0                                                      | General.....                                                        | 112        |
| K.1.2.1                                                      | Assessment of ACM-listed cryptographic mechanisms.....              | 112        |
| K.1.2.1.1                                                    | Assessment objective .....                                          | 112        |
| K.1.2.1.2                                                    | Assessment preparation.....                                         | 112        |
| K.1.2.1.3                                                    | Assessment activities .....                                         | 112        |
| K.1.2.1.4                                                    | Assessment evidence.....                                            | 112        |
| K.1.2.1.5                                                    | Assessment verdict.....                                             | 113        |
| K.1.2.2                                                      | Assessment of ACM-extended cryptographic mechanisms.....            | 113        |
| K.1.2.2.1                                                    | Assessment objective .....                                          | 113        |
| K.1.2.2.2                                                    | Assessment preparation.....                                         | 113        |
| K.1.2.2.3                                                    | Assessment activities .....                                         | 113        |
| K.1.2.2.4                                                    | Assessment evidence.....                                            | 114        |
| K.1.2.2.5                                                    | Assessment verdict.....                                             | 114        |
| K.1.2.3                                                      | Assessment of interoperability-based cryptographic mechanisms.....  | 114        |
| K.1.2.3.1                                                    | Assessment objective .....                                          | 114        |
| K.1.2.3.2                                                    | Assessment preparation.....                                         | 114        |
| K.1.2.3.3                                                    | Assessment activities .....                                         | 114        |
| K.1.2.3.4                                                    | Assessment evidence.....                                            | 115        |
| K.1.2.3.5                                                    | Assessment verdict.....                                             | 115        |
| K.2                                                          | Crypto agility.....                                                 | 115        |
| K.2.1                                                        | Requirement .....                                                   | 115        |
| K.2.2                                                        | Assessment of crypto-agility .....                                  | 116        |
| K.2.2.1                                                      | Assessment objective.....                                           | 116        |
| K.2.2.2                                                      | Assessment preparation .....                                        | 116        |
| K.2.2.3                                                      | Assessment activities .....                                         | 117        |
| K.2.2.4                                                      | Assessment evidence .....                                           | 117        |
| K.2.2.5                                                      | Assessment verdict .....                                            | 117        |
| K.3                                                          | ACM-extended cryptographic mechanisms .....                         | 117        |
| K.3.1                                                        | Requirement .....                                                   | 117        |
| K.3.2                                                        | List of ACM-extended cryptographic mechanisms.....                  | 118        |
| K.3.3                                                        | Assessment.....                                                     | 118        |
| K.4                                                          | Interoperability-based cryptographic mechanisms.....                | 118        |
| K.4.1                                                        | Requirement .....                                                   | 118        |
| K.4.2                                                        | List of interoperability-based cryptographic mechanisms.....        | 118        |
| K.4.3                                                        | Assessment.....                                                     | 118        |
| <b>Annexes I to T: Void.....</b>                             |                                                                     | <b>119</b> |
| <b>Annex U (informative):      Use case description.....</b> |                                                                     | <b>120</b> |
| U.1                                                          | UC1 - Product for use in Private PKI for non critical sectors ..... | 120        |
| U.1.1                                                        | UC1 - General description.....                                      | 120        |
| U.1.2                                                        | UC1 - Product Functions and assets .....                            | 122        |
| U.1.2.1                                                      | UC1 - List of functions .....                                       | 122        |
| U.1.2.2                                                      | UC1 - Assets .....                                                  | 123        |
| U.1.3                                                        | UC1 - Operational Environment .....                                 | 123        |
| U.1.4                                                        | UC1 - Distribution of Security Functions.....                       | 123        |
| U.1.5                                                        | UC1 - Users.....                                                    | 124        |
| U.2                                                          | UC2 - Product for use in Private PKI for critical entities.....     | 124        |
| U.2.1                                                        | UC2 - General description.....                                      | 124        |
| U.2.2                                                        | UC2 - List of functions.....                                        | 126        |
| U.2.2.1                                                      | UC2 - Assets .....                                                  | 127        |
| U.2.3                                                        | UC2 - Operational Environment .....                                 | 127        |
| U.2.4                                                        | UC2 - Distribution of Security Functions.....                       | 128        |
| U.2.5                                                        | UC2 - Users.....                                                    | 128        |
| U.3                                                          | UC3 - Public PKI for critical entities .....                        | 128        |
| U.3.1                                                        | General description.....                                            | 128        |

|                               |                                                             |            |
|-------------------------------|-------------------------------------------------------------|------------|
| U.3.2                         | UC3 - List of functions.....                                | 129        |
| U.3.2.1                       | UC3 - Assets .....                                          | 130        |
| U.3.3                         | UC3 - Operational Environment .....                         | 130        |
| U.3.4                         | UC3 - Distribution of Security Functions.....               | 131        |
| U.3.5                         | UC3 - Users.....                                            | 131        |
| U.4                           | UC4 - Product for use in Critical Public basic PKI.....     | 131        |
| U.4.1                         | UC4 - General description.....                              | 131        |
| U.4.2                         | UC4 - List of functions.....                                | 133        |
| U.4.2.1                       | UC4 - Assets .....                                          | 133        |
| U.4.3                         | UC4 - Operational Environment .....                         | 134        |
| U.4.4                         | UC4 - Distribution of Security Functions.....               | 134        |
| U.4.5                         | UC4 - Users .....                                           | 134        |
| U.5                           | UC5 - Product for use in Critical Multi-Authority PKI ..... | 134        |
| U.5.1                         | General description.....                                    | 134        |
| U.5.2                         | UC5 - List of functions.....                                | 136        |
| U.5.2.1                       | UC5 - Assets .....                                          | 137        |
| U.5.3                         | UC5 - Operational Environment .....                         | 138        |
| U.5.4                         | UC5 - Distribution of Security Functions.....               | 138        |
| U.5.5                         | UC5 - Users .....                                           | 138        |
| <b>Annex V (informative):</b> | <b>Change history .....</b>                                 | <b>139</b> |
| History .....                 |                                                             | 141        |

# Sample Document

get full document from [standards.iteh.ai](https://standards.iteh.ai)

---

# Intellectual Property Rights

## Essential patents

IPRs essential or potentially essential to normative deliverables (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)) may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the [ETSI IPR online database](#).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

## Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

---

## Foreword

This draft Harmonised European Standard (EN) has been produced by ETSI Technical Committee Cyber Security (CYBER), and is now submitted for the combined Public Enquiry and Vote phase of the ETSI Standardisation Request deliverable Approval Procedure (SRdAP).

The present document has been prepared under the Commission's Standardisation request M/606 - C(2025)618 [i.3] to provide one voluntary means of conforming to the requirements of EU Regulation No 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) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (CRA) [i.1].

Once the present document is cited in the Official Journal of the European Union under that Regulation, compliance with the normative clauses of the present document given in Table A.1 confers, within the limits of the scope of the present document, a presumption of conformity with the corresponding requirements of that Regulation and associated EFTA regulations.

| Proposed national transposition dates                                                  |                                 |
|----------------------------------------------------------------------------------------|---------------------------------|
| Date of latest announcement of this EN (doa):                                          | 3 months after ETSI publication |
| Date of latest publication of new National Standard or endorsement of this EN (dop/e): | 6 months after doa              |
| Date of withdrawal of any conflicting National Standard (dow):                         | 18 months after doa             |

---

## Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

---

## Introduction

The present document provides the technical cybersecurity requirements for the products in scope, following a risk-based approach in support of the Cyber Resilience Act (CRA) [i.1]. The technical cybersecurity requirements are thereby proportionate to the intended purpose, reasonably foreseeable use, deployment context, and threat exposure of the products.

Clause 4 does not contain technical requirements; it describes the product context that is considered for the application of the present document.

Clause 4 also defines Use Cases (UCs) that represent the main deployment scenarios reflecting the intended purpose and reasonably foreseeable use of the product, which serve as the basis for identifying relevant cybersecurity risks.

Clause 5 specifies technical cybersecurity requirements for the product to mitigate the identified risks, including their applicability conditions.

Clause 6 specifies the assessment criteria and compliance verification procedures with the requirements of Clause 5.

Annex A maps the technical requirements of the present document with the essential requirements of the CRA [i.1] regulation.

Annex B informs about the methodology used to assess the security risks of the products in their context.

Annex K supports the definition of the cryptographic requirements and assessment criteria used by the present document.

Annex U defines in more details the use cases contexts and parameters.

---

# 1 Scope

The present document specifies technical requirements and corresponding assessment criteria for public key infrastructure and digital certificate issuance software related to cybersecurity. The products with digital elements in scope, thereafter "the Products":

- are specified within the "technical description" of the "category of product" number "9" by the Commission Implementing Regulation (EU) 2025/2392 [i.2] as:  
"Products with digital elements used as part of a public key infrastructure (PKI) that manage the validation, creation, issuance, distribution, status publication, renewal or revocation of digital certificates, or the generation, storage, escrow, exchange, destruction or rotation of cryptographic keys associated with such digital certificates. This category includes but is not limited to key management systems, digital certificate management systems, online certificate status protocol responders and all-in-one PKI solutions".
- are only covered within the product context described in clause 4.

The present document covers those Products to demonstrate compliance with essential cybersecurity requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I under the conditions identified in annex A.

Different use cases representing different product architecture are presented in clause 4.6. Requirements applicability in clause 5 then defines which requirements apply to which use case to ensure compliance with the CRA's essential cybersecurity requirements.

---

# 2 References

## 2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found in the [ETSI docbox](#).

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are necessary for the application of the present document.

- [1] ENISA Report 1747792503: "[European Cybersecurity Certification Group Sub-group on Cryptography Agreed Cryptographic Mechanisms](#) - version 2" – April 2025.
- [2] [Recommendation ITU-T X.509 \(10/2019\)](#): "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

NOTE: Identical text in the defining of public-key and attribute certificates is also available in ISO/IEC 9594-8 (paywall).

- [3] [IEEE Std 1609.2™-2025](#) "(2025)": "Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages".
- [4] [IETF RFC 6960](#) (June 2013): "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

## 2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or nonspecific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding but are not required for conformance to the present document.

- [i.1] [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).
- [i.2] [Commission Implementing Regulation \(EU\) 2025/2392](#) of 28 November 2025 on the technical description of the categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of the Council.
- [i.3] [Standardisation request M/606 - C\(2025\)618](#): "Commission Implementing decision of 3.2.2025 on a standardisation request to the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications Standards Institute (ETSI) as regards products with digital elements in support of 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)".
- [i.4] prEN 40000-1-1: "Cybersecurity requirements for products with digital elements - Vocabulary", produced by CEN CENELEC.

NOTE: Version and date to be added upon its publication by CEN CENELEC.

- [i.5] IETF RFC 4120: "The Kerberos Network Authentication Service (V5) - July 2005".
- [i.6] ETSI GS NFV 003 (V1.4.1) (2018-08): "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".
- [i.7] ETSI TS 102 941 (V2.2.1) (11-2022): "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management; Release 2".
- [i.8] ETSI TS 102 165-2 (V4.2.1): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures".
- [i.9] ETSI TS 133 501: "5G; Security architecture and procedures for 5G System (3GPP TS 33.501). .
- [i.10] ETSI EN 319 411-1 (V1.5.1) (04-2025): "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".
- [i.11] [EU C-ITS Certificate policy](#).
- [i.12] [EU C-ITS Security Policy](#).
- [i.13] [Directive \(EU\) 2023/2661](#) of the European Parliament and of the Council of 22 November 2023 amending Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport. .
- [i.14] ETSI TS 103 097: "Intelligent Transport Systems (ITS); Security; Security header and certificate formats; Release 2".
- [i.15] ETSI TR 119 540 (V1.1.1) (10-2025): "Electronic Signatures and Trust Infrastructures (ESI); Standardization requirements for Smart Contracts based on Electronic Ledgers".
- [i.16] ETSI TS 102 940 (V2.1.1) (07-2021): "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management; Release 2".
- [i.17] prEN 40000-1-3: "Cybersecurity requirements for products with digital elements – Vulnerability Handling", produced by CEN CENELEC. .

NOTE: Version and date to be added upon its publication by CEN CENELEC.

- [i.18] IETF RFC 5280: "Intelligent Transport Systems (ITS); Security; Security header and certificate formats; Release 2".
- [i.19] [Directive \(EU\) 2022/2557](#) of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC".
- [i.20] NIST SP 800-130: "A Framework for Designing Cryptographic Key Management Systems" - August 2013.
- [i.21] [Regulation \(EU\) 2016/679](#) of the European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

## 3 Definition of terms, symbols and abbreviations

### 3.1 Terms

For the purposes of the present document, the terms given in Regulation (EU) 2024/2847 [i.1], prEN 40000-1-1 [i.4] and the following apply:

**certificate:** public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it

NOTE: See ETSI EN 319 411-1 [i.10].

**Certificate Policy (CP):** named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

NOTE: See ETSI EN 319 411-1 [i.10].

**Certificate Revocation List (CRL):** signed list indicating a set of certificates that have been revoked by the certificate issuer.

NOTE: See ETSI EN 319 411-1 [i.10].

**Certification Authority (CA):** authority trusted by one or more users to create and assign certificates

NOTE: See ETSI EN 319 411-1 [i.10].

**critical entities:** critical entities as defined by Directive (EU) 2022/2557.

NOTE: See [Directive \(EU\) 2022/2557 – Resilience of Critical Entities \(CER\)](#) [i.19].

**Cryptographic Key Management System (KMS):** Framework and services that provide for the generation, production, establishment, control, accounting, and destruction of cryptographic keys. It includes all elements (policies, procedures, devices, and components), facilities, personnel, and information products that form the system that establishes, manages, and supports cryptographic products and services for end entities.

NOTE: See NIST SP 800-130 [i.20].

**digital signature:** data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

NOTE: See ETSI EN 319 411-1 [i.10].

**personal data:** any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

NOTE: See [Regulation \(EU\) 2016/679 \(GDPR\)](#) [i.21].

**PKI Software:** software implementing the PKI services, including, Registration, Certificate generation, Dissemination, Revocation management, Certificate status, Logging of security events, User accounts management

**product:** product with Digital Elements in the scope of the present document

NOTE: [Cyber Resilience Act \(Regulation \(EU\) 2024/2847\)](#) [i.1].

**Registration Authority (RA):** entity that is responsible for identification and authentication of subjects of certificates mainly

NOTE: See ETSI EN 319 411-1 [i.10].

**secure cryptographic:** device which holds the user's private key, protects this key against compromise and performs signing or decryption functions on behalf of the user

NOTE: See ETSI EN 319 411-1 [i.10].

## 3.2 Symbols

Void.

## 3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

|       |                                                         |
|-------|---------------------------------------------------------|
| AA    | Authorisation Authority                                 |
| AE    | Authentication Entity                                   |
| AES   | Advanced Encryption Standard                            |
| AID   | Authentication Identifier                               |
| AP    | Access Point                                            |
| API   | Application Programming Interface                       |
| ARC   | Architecture                                            |
| AT    | Authorisation Ticket                                    |
| C-ITS | Cooperative ITS                                         |
| CA    | Certification Authority                                 |
| CARL  | Certification Authority Revocation List                 |
| CEN   | Comité Européen de Normalisation                        |
| COM   | Communications                                          |
| CP    | Certificate Policy                                      |
| CPOC  | C-ITS-Point of Contact                                  |
| CPS   | Certification Practice Statement                        |
| CRA   | Cyber Resilience Act                                    |
| CRL   | Certificate Revocation List                             |
| CRY   | Cryptography                                            |
| CSA   | Cybersecurity Act                                       |
| CSP   | Cloud Service Provider / Cryptographic Service Provider |
| CSR   | Certificate Signing Request                             |
| CTL   | Certificate Trust List                                  |
| DC    | Distribution Center                                     |
| EA    | Enrolment Authority (similar to LTCA)                   |
| EC    | Enrolment Credential (similar to LTC)                   |
| ECTL  | Extended Certificate Trust List                         |
| HMAC  | Hash-based Message Authentication Code                  |
| HMI   | Human-Machine Interface                                 |
| HSM   | Hardware Security Module                                |
| IEEE  | Institute of Electrical and Electronics Engineers       |
| IT    | Information Technology                                  |
| ITS   | Intelligent Transport System                            |
| KMS   | Key Management System                                   |
| LAN   | Local Area network                                      |
| MA    | Misbehaviour Authority                                  |

|       |                                    |
|-------|------------------------------------|
| NA    | National Accreditation             |
| CSP   | Online Certificate Status Protocol |
| PKC   | Public Key Certificate             |
| PKI   | Public Key Infrastructure          |
| POE   | Physical Operational Environment   |
| PP    | Protection Profile                 |
| RA    | Registration Authority             |
| RBAC  | Role-Based Access Control          |
| RCA   | Root Certificate Authority         |
| RCS   | Remote Control System              |
| SCD   | Secure Cryptographic Device        |
| SHA   | Secure Hash Algorithm              |
| SOE   | Software Operational Environment   |
| SOTA  | State of the Art                   |
| SP    | Security Profile                   |
| SSO   | Single Sign-on                     |
| SSP   | Service Specific Permission        |
| SubCA | Subordinate Certificate Authority  |
| TAE   | Target of Assessment               |
| TLM   | Trust List Manager                 |
| TLS   | Transport Layer Security           |
| TPM   | Trusted Platform Module            |
| TSL   | Trust-service Status List          |
| TSP   | Trust Service Provider             |
| UC    | Use Case                           |
| URL   | Uniform Resource Locator           |
| VCS   | Version Control System             |
| VPN   | Virtual Private Network            |

Sample Document

## 4 Product context

get full document from standards.iteh.ai

### 4.0 Introduction

The technical requirements of the present document apply under the product context described herein, which shall be in accordance with its intended use. The equipment shall comply with all the technical requirements of the present document at all times when operating in such product context.

A PKI is a system that enables the management of public keys, and requires that the private key is kept secret. The assurance of the secrecy of the private key is most often achieved by maintaining the secret key in a hardware security module and limiting access to the key to cryptographic functions in such a way that the secret key itself is never visible externally to the device. Assertions that are signed by the private key similarly require that only the device holding the private key is able to create the signature. Verifications of signed attestations need access to the public key of the signer, and often that public key is distributed in a Public Key Certificate (PKC) that is stored securely on the verifying device.

**NOTE:** A public key has limited security value as it is intended to be known to all, but the PKC may contain some identifying information and therefore the PKC content should be protected in accordance with any general data protection rules for personal, or Personal Identifying Information (PII).

The present document describes product contexts for products with digital elements used as part of a Public Key Infrastructure (PKI) that manage the validation, creation, issuance, distribution, status publication, renewal or revocation of digital certificates, or the generation, storage, escrow, exchange, destruction or rotation of cryptographic keys associated with such digital certificates.

The reasonably foreseeable use of the product is to support certification services where a compromise carries a significant risk of impact to the security of other products, networks or services, or to the health, security or safety of the public.

**EXAMPLE 1:** C-ITS. In the context of the present document ETSI TS 102 941 [i.7] and the EU C-ITS Certificate Management System policy [i.11] and security profile [i.12] documents identify specific requirements on hardware elements and their certification.