



**Cybersecurity (CYBER);
CRA;
Cybersecurity requirements for firewalls,
intrusion detection and/or prevention systems**

get full document from standards.iteh.ai

Reference

DEN/CYBER-EUS-0020

Keywords

CRA, cybersecurity, firewall

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

Intellectual Property Rights	8
Foreword.....	9
Modal verbs terminology	9
Introduction	9
1 Scope	10
2 References	11
2.1 Normative references	11
2.2 Informative references	11
3 Definition of terms, symbols and abbreviations.....	13
3.1 Terms	13
3.2 Symbols	15
3.3 Abbreviations.....	15
4 Product context.....	16
4.1 Introduction.....	16
4.2 Product functions.....	16
4.2.1 General product functions	16
4.2.1.1 General	16
4.2.1.2 [FN-G-01] Configuration and management	16
4.2.1.3 [FN-NC-01] Network connectivity	17
4.2.1.4 [FN-LG-01] Logging	17
4.2.1.5 [FN-TI-01] Traffic inspection and analysis	17
4.2.1.6 [FN-SM-01] Signature and intelligence management	17
4.2.2 Product functions implemented by firewalls and intrusion prevention systems.....	17
4.2.2.1 General	17
4.2.2.2 [FN-SP-01] Traffic access control and decision making	17
4.2.2.3 [FN-SG-01] Traffic segmentation	17
4.2.3 Product functions implemented by intrusion detection systems and intrusion prevention systems	17
4.2.3.1 General	17
4.2.3.2 [FN-TD-01] Threat detection and pattern matching	17
4.3 Product architecture	18
4.3.1 General	18
4.3.2 Product assets	18
4.3.3 Product capabilities	18
4.4 Operational environment	18
4.4.1 General description	18
4.4.2 Physical environment	18
4.4.3 Logical environment	19
4.4.4 Connectivity aspects.....	19
4.5 Distribution of security functions	19
4.6 Users	19
4.7 Use cases.....	20
4.7.1 General	20
4.7.2 Perimeter security deployments	20
4.7.3 Internal segmentation deployments.....	20
4.7.4 Data centre security deployments.....	20
4.7.5 Cloud security deployments	21
4.7.6 Distributed branch office protection.....	21
4.7.7 Network forensics deployments	21
4.7.8 Threat hunting deployments.....	21
4.7.9 Host-based security deployments.....	21
4.7.10 Application security deployments	21
4.7.11 Managed security service deployments.....	21
5 Technical requirements for the products	22

5.1	Introduction - Applicability of the requirements	22
5.2	Appropriate level of cybersecurity	22
5.3	No known exploitable vulnerabilities	22
5.3.1	[KEV-1] No known exploitable vulnerabilities	22
5.3.1.1	General	22
5.3.1.2	Requirements	22
5.4	Secure by default configuration	23
5.4.1	[DEFAULT-1] Secure by default configuration	23
5.4.1.1	General	23
5.4.1.2	Requirements	23
5.4.2	[RESET-1] Factory reset	24
5.4.2.1	General	24
5.4.2.2	Requirements	24
5.5	Security updates	24
5.5.1	[UPDATE-1] Update mechanisms	24
5.5.1.1	General	24
5.5.1.2	Requirements	24
5.6	Authentication and access control	25
5.6.1	[AUTH-1] Authentication	25
5.6.1.1	General	25
5.6.1.2	Requirements	25
5.6.2	[AUTH-2] Authorisation	26
5.6.2.1	General	26
5.6.2.2	Requirements	26
5.6.3	[AUTH-3] Authenticated session lifecycle	26
5.6.3.1	General	26
5.6.3.2	Requirements	26
5.6.4	[AUTH-4] Protocol access control	27
5.6.4.1	General	27
5.6.4.2	Requirements	27
5.7	Confidentiality protection	27
5.7.1	General	27
5.7.2	Requirements	28
5.8	Availability protection	28
5.8.1	General	28
5.8.2	Requirements	28
5.9	Non-interference	29
5.9.1	General	29
5.9.2	Requirements	29
5.10	Attack surface minimalisation	29
5.10.1	[INTEGRITY-1] System integrity and boot process	29
5.10.1.1	General	29
5.10.1.2	Requirements	29
5.10.2	[PACKET-1] Default packet disposition	30
5.10.2.1	General	30
5.10.2.2	Requirements	30
5.10.3	[EXPOSURE-1] Interface and service exposure minimisation	30
5.10.3.1	General	30
5.10.3.2	Requirements	30
5.11	Monitoring and logging	30
5.11.1	General	30
5.11.2	Requirements	30
5.12	Data management	31
5.12.1	[TRANSFER-1] Secure data export and transfer	31
5.12.1.1	General	31
5.12.1.2	Requirements	31
5.12.2	[SIGNATURE-1] Signature update and validation	31
5.12.2.1	General	31
5.12.2.2	Requirements	31
5.13	Remote data processing solutions	32
5.13.1	General	32
5.13.2	Requirements	32

6	Assessment criteria for compliance with technical requirements	33
6.1	Introduction to the assessment and compliance criteria	33
6.2	Appropriate level of cybersecurity	33
6.3	No known exploitable vulnerabilities	33
6.3.1	[KEV-1] No known exploitable vulnerabilities	33
6.3.1.1	Requirement assessments	33
6.4	Secure by default configuration	36
6.4.1	[DEFAULT-1] Secure by default configuration	36
6.4.1.1	Requirement assessments	36
6.4.2	[RESET-1] Factory reset	48
6.4.2.1	Requirement assessments	48
6.5	Security updates	51
6.5.1	[UPDATE-1] Update mechanisms	51
6.5.1.1	Requirement assessments	51
6.6	Authentication and access control	58
6.6.1	[AUTH-1] Authentication	58
6.6.1.1	Requirement assessments	58
6.6.2	[AUTH-2] Authorisation	66
6.6.2.1	Requirement assessments	66
6.6.3	[AUTH-3] Authenticated session lifecycle	70
6.6.3.1	Requirement assessments	70
6.6.4	[AUTH-4] Protocol access control	74
6.6.4.1	Requirement assessments	74
6.7	Confidentiality protection	79
6.7.1	Requirement assessments	79
6.8	Availability protection	85
6.8.1	Requirement assessments	85
6.9	Non-interference	88
6.9.1	Requirement assessments	88
6.10	Attack surface and mitigation	90
6.10.1	[INTEGRITY-1] System integrity and boot process	90
6.10.1.1	Requirement assessments	90
6.10.2	[PACKET-1] Default packet disposition	94
6.10.2.1	Requirement assessments	94
6.10.3	[EXPOSURE-1] Interface and service exposure minimisation	99
6.10.3.1	Requirement assessments	99
6.11	Monitoring and logging	102
6.11.1	Requirement assessments	102
6.12	Data management	105
6.12.1	[TRANSFER-1] Secure data export and transfer	105
6.12.1.1	Requirement assessments	105
6.12.2	[SIGNATURE-1] Signature update and validation	109
6.12.2.1	Requirement assessments	109
6.13	Remote data processing solutions	115
6.13.1	Requirement assessments	115

Annex A (informative):	Relationship between the present document and the essential cybersecurity requirements of EU Regulation (EU) 2024/2847	120
-------------------------------	---	------------

Annex B (informative):	Security analysis	122
-------------------------------	--------------------------------	------------

B.1	General	122
B.2	Threat landscape	122
B.2.1	Threats related to vulnerability handling	122
B.2.2	Threats related to access control and authentication	123
B.2.3	Threats related to availability and inspection bypass	123
B.2.4	Threats related to integrity and tampering	124
B.2.5	Threats related to signature and intelligence integrity	124
B.2.6	Threats related to data protection	125
B.2.7	Threats related to monitoring and visibility	125
B.2.8	Threats related to default configuration	125

B.2.9	Threats related to physical and deployment security	126
B.2.10	Threats related to detection disruption	126
B.3	Threat assessment framework	126
B.3.1	Introduction	126
B.3.2	Risk factors	127
B.3.2.0	Introduction	127
B.3.2.1	Baseline risk factors	127
B.3.2.2	Traffic inspection risk factors	128
B.3.2.3	Update and intelligence risk factors	128
B.3.2.4	Deployment architecture risk factors	128
B.3.2.5	Data operations risk factors	128
B.3.2.6	Remote data processing risk factors	129
B.3.3	Threat justification and mitigation	129
Annexes C to J: Void		133
Annex K (normative): Vertical specific state of the art cryptography		134
K.0	General	134
K.1	Classification of cryptographic algorithms as CRY-SOTA	134
K.2	Assessment criteria for compliance with cryptographic requirements	135
K.2.1	Assessment objective	135
K.2.2	Assessment preparation	135
K.2.3	Assessment activities	135
K.2.4	Assessment evidence	136
K.2.5	Assessment verdict	137
K.3	Symmetric atomic primitives	137
K.3.1	Block ciphers	137
K.3.2	Stream ciphers	138
K.3.3	Hash functions	138
K.4	Symmetric constructions	138
K.4.1	Confidentiality modes of operation: encryption/decryption modes	138
K.4.2	Specific confidentiality modes: disk encryption	138
K.4.3	Integrity modes: message authentication codes	139
K.4.4	Symmetric entity authentication schemes	139
K.4.5	Authenticated encryption	139
K.4.6	Key protection	139
K.4.7	Key derivation functions	139
K.4.8	Password protection/password hashing mechanisms	139
K.4.9	Key combiners	140
K.5	Asymmetric atomic primitives	140
K.5.1	RSA/Integer factorisation	140
K.5.2	Discrete logarithm in finite fields	140
K.5.3	Discrete logarithm in elliptic curves	140
K.5.4	Learning with errors in (structured) lattices	140
K.5.5	Hash function preimage resistance	140
K.5.6	Other intractable problems	140
K.6	Asymmetric constructions	141
K.6.1	Asymmetric encryption scheme	141
K.6.2	Digital signature	141
K.6.3	Asymmetric entity authentication schemes	141
K.6.4	Key establishment and key encapsulation	141
K.7	Cryptographic protocols	141
K.7.1	QUIC	141
K.7.2	SNMP	142
K.7.3	Secure device identity	142
K.7.4	Time Protocols	142

K.8	Cryptographic industry standards.....	143
K.9	Crypto agility	143
K.9.1	Requirement.....	143
K.9.2	Assessment of crypto-agility.....	144
K.9.2.1	Assessment objective	144
K.9.2.2	Assessment preparation.....	144
K.9.2.3	Assessment activities.....	144
K.9.2.4	Assessment evidence.....	144
K.9.2.5	Assessment verdict.....	145
History		146

Sample Document

get full document from 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.

Sample Document

get full document from standards.iteh.ai

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 C(2025)618 final [i.3] to provide one voluntary means of conforming to the requirements 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) (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 covers cybersecurity for firewalls, intrusion detection systems, and intrusion prevention systems. These products are identified in Annex III, Class II, point 2 of Regulation (EU) 2024/2847 [i.1], known as the Cyber Resilience Act (CRA).

The present document provides a structured approach to identify the applicable cybersecurity requirements for the products in scope, following a risk-based approach. Security controls are therefore proportionate to the intended purpose, reasonably foreseeable use, deployment context, and threat exposure of the products.

Clause [4](#) describes the product architecture and intended purpose, and defines the use cases for the main deployment scenarios under reasonably foreseeable use.

Clause [5](#) specifies the technical cybersecurity requirements for the product to mitigate the identified risks.

Clause [6](#) specifies the assessment criteria and compliance verification procedures for the requirements of clause [5](#).

Annex [A](#) maps the technical requirements of the present document to the corresponding cybersecurity requirements of the CRA [i.1].

Annex [B](#) describes the methodology used to assess the security risks of the products in their context. Where a product does not clearly correspond to one of the use cases defined in clause [4](#), the risk assessment methodology of Annex [B](#) may be used to determine the applicable cybersecurity requirements.

1 Scope

The present document specifies vulnerability handling activities, technical requirements and corresponding assessment criteria for firewalls, intrusion detection systems, and intrusion prevention systems related to cybersecurity. The products with digital elements in scope:

- are specified within the "technical description" of the "category of product" in Class II, point 2 by the Commission Implementing Regulation (EU) 2025/2392 [i.2] 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.1] as:
 - "Firewalls are products with digital elements that protect a connected network or system from unauthorised access by monitoring and restricting data communication traffic to and from that network.

This category includes but is not limited to network firewalls and application firewalls such as web application firewalls or filters and anti-spam gateways.";
 - "Intrusion detection systems are products with digital elements that monitor traffic once it has entered the network environment for suspicious activity and detect or identify that an intrusion has been attempted, is occurring, or has occurred on a connected network or system.

This category includes but is not limited to network-based intrusion detection systems and host-based intrusion detection systems.";
 - "Intrusion prevention systems are products with digital elements composed of an intrusion detection system that actively responds to an intrusion to a connected network or system.

This category includes but is not limited to network-based intrusion prevention systems and host-based intrusion prevention systems.";
- are only covered within the product context described in clause 4.

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

Firewalls, intrusion detection systems, and intrusion prevention systems fall within the scope of the present document, whether deployed as physical appliances or software. The present document applies when the intended purpose or reasonably foreseeable use involves monitoring, analysing, or controlling network traffic for security purposes. Products that detect access attempts made without authorisation, identify malicious activity, or enforce traffic controls to protect networks and systems from intrusions are within scope.

Firewalls, intrusion detection systems, and intrusion prevention systems intended for use in the industrial OT (Operational Technology) domain are excluded from the scope of the present document, see prEN 50770-1 [i.7].

The present document does not specify how products detect threats, classify traffic, or implement inspection algorithms. Detection accuracy rates, false positive thresholds, and signature effectiveness metrics are outside scope. Security requirements for the robustness of protocol parsing engines, the integrity of inspection processes, and vulnerability management remain within scope.

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 European Cybersecurity Certification Group, Sub-group on Cryptography: "[Agreed Cryptographic Mechanisms](#)", Version 2.0, April 2025.
- [2] [ETSI TS 119 312 \(V2.1.1\) \(06-2026\)](#): "Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites".
- [3] [ETSI TS 133 210 \(V19.3.0\) \(02-2026\)](#): "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210 version 19.3.0 Release 19)".

2.2 Informative 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.

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] NIST SP 800-133 Rev. 2 (June 2020): "Recommendation for Cryptographic Key Generation".

- [i.6] ISO/IEC/IEEE 24765:2017: "Systems and software engineering - Vocabulary".
- [i.7] prEN 50770-1: "Security for Operational Technologies - Part 1: Security Profile for firewalls and intrusion detection and prevention systems", (produced by CEN CENELEC).

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

- [i.8] [ENISA European Vulnerability Database \(EUVD\), established pursuant to Article 12\(2\) of Directive \(EU\) 2022/2555.](#)
- [i.9] [ENISA: "Single Reporting Platform \(SRP\)" established for Regulation \(EU\) 2024/2847.](#)
- [i.10] [BSI TR-02102-1](#) (Version 2026-01, 31 January 2026): "Cryptographic Mechanisms: Recommendations and Key Lengths".
- [i.11] ANSSI Référentiel Général de Sécurité, Annex B2: "[Choice and Sizing of Cryptographic Mechanisms](#)".
- [i.12] [Canadian Centre for Cyber Security ITSP.40.062](#): "Guidance on Securely Configuring Network Protocols".
- [i.13] [NIST SP 800-131A Rev. 2 \(March 2019\)](#): "Transitioning the Use of Cryptographic Algorithms and Key Lengths".
- [i.14] Arm Limited: "[Arm CCA Security Model 1.0](#)" (DEN0096).
- [i.15] [IRTF RFC 8439](#): "ChaCha20 and Poly1305 for IETF Protocols".
- [i.16] [IETF RFC 4418](#): "UMAC: Message Authentication Code using Universal Hashing".
- [i.17] [IETF RFC 9106](#): "Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications".
- [i.18] [IETF RFC 7914](#): "The scrypt Password-Based Key Derivation Function".
- [i.19] [IETF RFC 8410](#): "Algorithm Identifiers for Ed25519, Ed448, X25519, and X448 for Use in the Internet X.509 Public Key Infrastructure".
- [i.20] [IRTF RFC 8032](#): "Edwards-Curve Digital Signature Algorithm (EdDSA)".
- [i.21] [IETF RFC 8420](#): "Using the Edwards-Curve Digital Signature Algorithm (EdDSA) in the Internet Key Exchange Protocol Version 2 (IKEv2)".
- [i.22] [IETF RFC 9000](#): "QUIC: A UDP-Based Multiplexed and Secure Transport".
- [i.23] [IETF RFC 3411](#): "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks".
- [i.24] [IETF RFC 5590](#): "Transport Subsystem for the Simple Network Management Protocol (SNMP)".
- [i.25] [IEEE 802.1AR™-2018](#): "IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity".
- [i.26] [IEEE 1588™-2019](#): "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems".
- [i.27] [IETF RFC 8915](#): "Network Time Security for the Network Time Protocol".
- [i.28] [BSI TR-02102-2 \(Version 2026-01\)](#): "Cryptographic Mechanisms: Recommendations and Key Lengths - Use of Transport Layer Security (TLS)".
- [i.29] [BSI TR-02102-3 \(Version 2026-01\)](#): "Cryptographic Mechanisms: Recommendations and Key Lengths - Use of Internet Protocol Security (IPsec) and Internet Key Exchange (IKEv2)".
- [i.30] [BSI TR-02102-4 \(Version 2026-01\)](#): "Cryptographic Mechanisms: Recommendations and Key Lengths - Use of Secure Shell (SSH)".

- [i.31] [IEEE 802.11™-2024](#): "IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

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:

audit event: timestamped, structured record of activities including authentication attempts, configuration changes, and product errors

critical security parameter: confidential information whose disclosure or modification can compromise product security

EXAMPLE: Secret cryptographic keys, authentication values such as passwords, PINs, private components of certificates.

cryptographic algorithm: sequence of instructions based on mathematical properties to protect confidentiality, integrity or authenticity against attacks

diagnostic: pertaining to the detection and isolation of faults or failures

NOTE: As defined in ISO/IEC/IEEE 24765 [i.6], clause 3.1190.

diagnostic interface: interface used for diagnostic or troubleshooting purposes, not part of the intended function of the product

EXAMPLE: UART, JTAG, and SWD.

factory reset: mechanism that restores the product to product factory default state

fail-open operation: operation of the product in which traffic that cannot be inspected is forwarded without applying a fail-secure action

NOTE: Fail-open operation can result from software configuration, hardware bypass, inspection or signature update windows, or per-flow bypass configuration.

fail-secure action: configured action applied by the product to traffic that cannot be inspected, such that the traffic is not forwarded without inspection

NOTE: Typical fail-secure actions include drop, block, reject, and quarantine.

firewalls: products with digital elements that protect a connected network or system from access made without authorisation by monitoring and restricting data communication traffic to and from that network or between nodes of that network

NOTE: This includes but is not limited to network firewalls and application firewalls such as Web Application Firewalls (WAF), anti-spam gateways and content filtering systems.

firmware: software stored in non-volatile memory that controls product operation

NOTE 1: Firmware includes boot sequences, operating system components, inspection engines, and management interfaces.

NOTE 2: Firmware can include persistent configuration data required for product operation.

intrusion detection systems: products with digital elements that monitor traffic once it has entered the network environment for suspicious activity and detect or identify that an intrusion has been attempted, is occurring, or has occurred on a connected network or system

NOTE: This includes but is not limited to network-based intrusion detection systems and host-based intrusion detection systems.

intrusion prevention systems: products with digital elements composed of an intrusion detection system that actively responds to an intrusion to a connected network or system

NOTE: This includes but is not limited to network-based intrusion prevention systems and host-based intrusion prevention systems.

legacy protocol: network protocol whose specification lacks state of the art cryptography to ensure the authenticity, integrity or confidentiality of security-relevant exchanges, where a secure alternative protocol or profile is widely available, and which is retained in the product exclusively to maintain interoperability with deployed systems

EXAMPLE: Protocols whose role is limited to local IP address configuration, local neighbour and address discovery, and name and service resolution are not considered legacy protocols for the purposes of the present document, irrespective of their cryptographic properties. These protocols are designed under explicit assumptions that specific risks are managed by the operational environment in which they are deployed, and are required for basic network attachment and reachability.

NOTE: A vulnerability in a specific implementation of a protocol does not, by itself, make the protocol a legacy protocol. Vulnerabilities associated with a legacy protocol can originate in its specification, in a specific implementation, or in both.

legacy system: system that operates using at least one legacy protocol

management override: deliberate configuration action by a privileged management account that (i) enables a non-default product behaviour; and (ii) is distinguishable from routine product configuration

NOTE: Mechanisms that satisfy management override include confirmation prompts acknowledging the consequence of the override, reauthentication for the override action, and separate management workflows for non-default behaviours. Default configuration values and settings inherited from templates are not management overrides.

network interface: physical interface that can be used to access the functionality of firewall, IDS or IPS via a network

product: firewall, intrusion detection system, or intrusion prevention system within the scope of the present document

product factory default state: state of the product as provided after manufacturing, reflecting the default configuration established by the manufacturer, to which the product returns after a factory reset

NOTE 1: Depending on the product design and business model, security functionalities, for example secure boot, trust anchors, or security policies, can be enabled by the manufacturer prior to delivery, or activated and configured by the customer or authorised operator during initial setup.

NOTE 2: The product can be delivered by the manufacturer to an importer or distributor that subsequently sells it to customers or puts it into service. In that case additional steps, for example finalisation of configuration, can be required before the product enters an operational state.

product operational state: state in which the product can operate within its intended purpose and reasonably foreseeable use with its current active configuration, whether this configuration corresponds to the preconfigured default settings or has been modified by the user

remote data processing solution: data processing at a distance for which the software is designed and developed by the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent the product from performing one of its functions

NOTE: As defined in Regulation (EU) 2024/2847, Article 3, point 2 [i.1].

reboot: specific management operation or autonomous reaction to product state that triggers a product restart

secure channel: path for transferring data between two entities or components that ensures confidentiality, integrity, and replay protection, as well as mutual authentication between the entities or components

NOTE 1: The secure channel can be provided using cryptographic, physical, or procedural methods or a combination thereof.

NOTE 2: As defined in NIST SP 800-133 Rev. 2 [i.5].

secure-by-default configuration: configuration in which the product satisfies requirements in clause [5.4.1](#)

security rule: specific statement or entry that specifies source, destination, protocol, port, action, and matching criteria for traffic classification

NOTE: Multiple rules can collectively express a single set of security decisions.

signature database: collection of patterns, heuristics, and indicators used by the product to detect known threats during traffic inspection

software bill of materials: formally structured list of all software components, libraries, and dependencies included in the product, with version identifiers

3.2 Symbols

Void.

3.3 Abbreviations

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

ACM	Agreed Cryptographic Mechanisms
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
API	Application Programming Interface
CAVP	Cryptographic Algorithm Validation Program
CCA	Confidential Compute Architecture
CFB	Cipher Feedback
CRA	Cyber Resilience Act
CTR	Counter
DMZ	DeMilitarised Zone
DoS	Denial of Service
EAP	Extensible Authentication Protocol
ECDSA	Elliptic Curve Digital Signature Algorithm
EdDSA	Edwards-curve Digital Signature Algorithm
EU	European Union
EUVD	European Vulnerability Database
GMAC	Galois Message Authentication Code
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IPR	Intellectual Property Rights
IPS	Intrusion Prevention System
ISO	International Organisation for Standardisation
ISP	Internet Service Provider
IT	Information Technology
ITSP	Information Technology Security Publication
JTAG	Joint Test Action Group
KDF	Key Derivation Function
LWE	Learning With Errors
MiB	Mebibyte
NTP	Network Time Protocol
NTS	Network Time Security
PAC	Pointer Authentication Code
PTP	Precision Time Protocol
QUIC	Quick UDP Internet Connections
RDPS	Remote Data Processing Solution