



**Cyber Security (CYBER);
CRA;
Cybersecurity requirements for routers, modems intended for
the connection to the internet and switches**

get full document from standards.iteh.ai

Reference

DEN/CYBER-EUS-0013

Keywords

CRA, cybersecurity, modem, router, switch

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 authorisation 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	12
3 Definition of terms, symbols and abbreviations.....	14
3.1 Terms	14
3.2 Symbols	15
3.3 Abbreviations.....	16
4 Product context.....	17
4.1 Introduction.....	17
4.2 Product functions.....	17
4.2.1 General product functions	17
4.2.1.1 General	17
4.2.1.2 [FN-G-01] Configuration and management	18
4.2.1.3 [FN-G-02] Monitoring and diagnostics	18
4.2.1.4 [FN-G-03] Access control	18
4.2.2 Product functions implemented by routers and switches	18
4.2.2.1 General	18
4.2.2.2 [FN-RS-01] Topology discovery	18
4.2.2.3 [FN-RS-02] Handling of network traffic processing rules	18
4.2.2.4 [FN-RS-03] Traffic access control	18
4.2.3 Product functions implemented by routers.....	18
4.2.3.1 General	18
4.2.3.2 [FN-R-01] Routing	18
4.2.3.3 [FN-R-02] WAN connectivity	18
4.2.4 Product functions implemented by switches	19
4.2.4.1 General	19
4.2.4.2 [FN-S-01] Switching	19
4.2.5 Product functions implemented by modems intended for connection to the internet.....	19
4.2.5.1 General	19
4.2.5.2 [FN-M-01] WAN connectivity	19
4.2.5.3 [FN-M-02] ISP-side remote management	19
4.2.6 Additional product capabilities	19
4.3 Product architecture	19
4.3.1 Product assets.....	19
4.4 Operational environment	21
4.4.1 General description	21
4.4.1.1 General	21
4.4.1.2 Residential deployments.....	21
4.4.1.3 Small enterprise deployments.....	21
4.4.1.4 Medium enterprise deployments.....	21
4.4.1.5 Large enterprise deployments.....	22
4.4.1.5.1 General.....	22
4.4.1.5.2 Data centre deployments.....	23
4.4.1.5.3 Service provider and carrier networks	23
4.4.2 Physical environment	23
4.4.3 Logical environment	23
4.4.4 Connectivity aspects.....	23
4.5 Distribution of security functions	24
4.6 Users	24

4.6.1	General	24
4.6.2	Natural persons.....	24
4.6.3	Legal entities	25
4.6.4	Devices.....	25
4.7	Use cases.....	25
4.7.1	General	25
4.7.2	Basic use cases	25
4.7.2.1	Physical devices for non-professional use	25
4.7.2.2	Physical devices for professional use	25
4.7.2.3	Routers and switches provided as virtual network functions.....	25
4.7.3	Supplementary use cases	26
4.7.3.1	Internet-facing enterprise edge devices	26
4.7.3.2	Devices within critical infrastructure.....	26
4.7.3.3	Devices within service provider and carrier network infrastructure	26
4.7.3.4	Devices serving persons with special protection needs	26
5	Technical requirements for products	26
5.1	Introduction - Applicability of the requirements	26
5.2	Appropriate level of cybersecurity.....	26
5.3	No known exploitable vulnerabilities	27
5.3.1	[KEV-1] No known exploitable vulnerabilities	27
5.3.1.1	General	27
5.3.1.2	Requirements	27
5.4	Secure by default configuration	27
5.4.1	[DEFAULT-1] Secure by default configuration	27
5.4.1.1	General	27
5.4.1.2	Requirements	27
5.4.2	[RESET-1] Factory reset.....	28
5.4.2.1	General	28
5.4.2.2	Requirements	28
5.5	Security updates	29
5.5.1	[UPDATE-1] Update mechanisms	29
5.5.1.1	General	29
5.5.1.2	Requirements	29
5.6	Authentication and access control	29
5.6.1	[AUTH-1] Authentication	29
5.6.1.1	General	29
5.6.1.2	Requirements	30
5.6.2	[AUTH-2] Authorisation	30
5.6.2.1	General	30
5.6.2.2	Requirements	30
5.6.3	[AUTH-3] Authenticated session lifecycle	31
5.6.3.1	General	31
5.6.3.2	Requirements	31
5.6.4	[AUTH-4] Protocol access control	31
5.6.4.1	General	31
5.6.4.2	Requirements	31
5.7	Confidentiality protection	32
5.7.1	General	32
5.7.2	Requirements.....	32
5.8	Availability and resilience	33
5.8.1	General	33
5.8.2	Requirements.....	33
5.9	Attack surface and mitigation	33
5.9.1	[INTEGRITY-1] System integrity and boot process.....	33
5.9.1.1	General	33
5.9.1.2	Requirements	34
5.9.2	[PACKET-1] Default packet disposition.....	34
5.9.2.1	General	34
5.9.2.2	Requirements	34
5.9.3	[EXPOSURE-1] Interface and service exposure minimisation.....	35
5.9.3.1	General	35

5.9.3.2	Requirements	35
5.10	Monitoring and logging	35
5.10.1	General	35
5.10.2	Requirements	35
5.11	Data management	35
5.11.1	[TRANSFER-1] Secure data export and transfer	35
5.11.1.1	General	35
5.11.1.2	Requirements	35
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	36
6.2.1	[KEV-1] No known exploitable vulnerabilities	36
6.2.1.1	Requirement assessments	36
6.3	Secure by default configuration	39
6.3.1	[DEFAULT-1] Secure by default configuration	39
6.3.1.1	Requirement assessments	39
6.3.2	[RESET-1] Factory reset	52
6.3.2.1	Requirement assessments	52
6.4	Security updates	55
6.4.1	[UPDATE-1] Update mechanisms	55
6.4.1.1	Requirement assessments	55
6.5	Authentication and access control	62
6.5.1	[AUTH-1] Authentication	62
6.5.1.1	Requirement assessments	62
6.5.2	[AUTH-2] Authorisation	70
6.5.2.1	Requirement assessments	70
6.5.3	[AUTH-3] Authenticated session lifecycle	74
6.5.3.1	Requirement assessments	74
6.5.4	[AUTH-4] Protocol access control	80
6.5.4.1	Requirement assessments	80
6.6	Confidentiality protection	85
6.6.1	Requirement assessments	85
6.7	Availability and resilience	91
6.7.1	Requirement assessments	91
6.8	Attack surface and mitigation	96
6.8.1	[INTEGRITY-1] System integrity and boot process	96
6.8.1.1	Requirement assessments	96
6.8.2	[PACKET-1] Default packet disposition	100
6.8.2.1	Requirement assessments	100
6.8.3	[EXPOSURE-1] Interface and service exposure minimisation	102
6.8.3.1	Requirement assessments	102
6.9	Monitoring and logging	104
6.9.1	Requirement assessments	104
6.10	Data management	108
6.10.1	[TRANSFER-1] Secure data export and transfer	108
6.10.1.1	Requirement assessments	108
Annex A (informative):	Relationship between the present document and the essential cybersecurity requirements of EU Regulation (EU) 2024/2847	113
Annex B (informative):	Security analysis	116
B.1	General	116
B.2	Threat landscape	117
B.2.1	Threats related to vulnerability handling	117
B.2.2	Threats related to packet processing and availability of services	118
B.2.3	Threats related to access control and authentication	120
B.2.4	Threats related to tampering and data processing	120
B.3	Threat assessment framework	122
B.3.1	Introduction	122

B.3.2	Risk factors	123
B.3.2.0	Introduction	123
B.3.2.1	Baseline risk factors	123
B.3.2.2	Management risk factors	124
B.3.2.3	Protocol implementation risk factors	124
B.3.2.4	Data operations risk factors	125
B.3.3	Threat justification and mitigation	125
Annexes C to J:	Void	129
Annex K (normative):	Generic requirements and assessment criteria for the use of state of the art cryptography	130
K.1	General	130
K.1.0	Introduction	130
K.1.1	Classification of cryptographic algorithms as CRY-SOTA	130
K.2	Assessment criteria for compliance with cryptographic requirements	131
K.2.0	Assessment objective	131
K.2.1	Assessment preparation	131
K.2.2	Assessment activities	131
K.2.3	Assessment evidence	132
K.2.4	Assessment verdict	133
K.3	Symmetric atomic primitives	133
K.3.0	Block ciphers	133
K.3.1	Stream ciphers	134
K.3.2	Hash functions	134
K.4	Symmetric constructions	134
K.4.0	Confidentiality modes of operation: encryption/decryption modes	134
K.4.1	Specific confidentiality modes: disk encryption	134
K.4.2	Integrity modes: message authentication codes	134
K.4.3	Symmetric entity authentication schemes	135
K.4.4	Authenticated encryption	135
K.4.5	Key protection	135
K.4.6	Key derivation functions	135
K.4.7	Password protection/password hashing mechanisms	135
K.4.8	Key combiners	136
K.5	Asymmetric atomic primitives	136
K.5.0	RSA/Integer factorization	136
K.5.1	Discrete logarithm in finite fields	136
K.5.2	Discrete logarithm in elliptic curves	136
K.5.3	Learning with errors in (structured) lattices	136
K.5.4	Hash function preimage resistance	137
K.5.5	Other intractable problems	137
K.6	Asymmetric constructions	137
K.6.0	Asymmetric encryption scheme	137
K.6.1	Digital signature	137
K.6.2	Asymmetric entity authentication schemes	137
K.6.3	Key establishment and key encapsulation	138
K.7	Cryptographic protocols	138
K.7.0	QUIC	138
K.7.1	MACSec	138
K.7.2	SNMP	139
K.7.3	Routing protocols	139
K.7.4	Secure device identity	139
K.7.5	Time Protocols	140
K.8	Cryptographic industry standards	140
K.9	Crypto agility	141

K.9.0	Requirement.....	141
K.9.1	Assessment of crypto-agility.....	141
K.9.1.1	Assessment objective	141
K.9.1.2	Assessment preparation.....	141
K.9.1.3	Assessment activities.....	142
K.9.1.4	Assessment evidence.....	142
K.9.1.5	Assessment verdict.....	142
History		143

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™** and **LTE™** 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 routers, modems intended for connection to the internet, and switches. These products are identified in Annex III, Class I, point 12 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 routers, modems intended for connection to the internet, and switches related to cybersecurity. The products with digital elements in scope:

- are specified within the "technical description" of the "category of product" in Class I, point 12 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:
 - "Routers are products with digital elements that establish and control the flow of data between different networks by selecting paths or routes using routing protocol mechanisms and algorithms, typically operating at the network layer.

This category includes but is not limited to wired and wireless routers, virtual routers and routers with or without modems.";
 - "Modems intended for the connection to the Internet are hardware products with digital elements that use digital modulation and demodulation techniques to convert analogue signals from and to digital signals for IP-based communication.

This category includes but is not limited to fibre modems, Digital Subscriber Line (DSL) modems, cable (DOCSIS) modems, satellite modems and cellular modems.";
 - "Switches are products with digital elements that provide connectivity between networked devices through traffic forwarding mechanisms typically implemented at the data link layer.

This category includes but is not limited to managed switches, smart switches, multilayer switches, virtual security switches, programmable switches for software-defined networking and bridges such as wireless access points.";
- 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.

NOTE 1: The term "internet" refers to any public network accessible beyond organizational boundaries. Public networks are accessible to multiple organizations or the general public. Private networks operate under single organizational control.

Routers, modems intended for connection to the internet, and switches fall within the scope of the present document when they provide management capabilities. This applies to all deployment forms such as dedicated hardware, virtual machines, containerized applications, and cloud-native network functions. The intended purpose or reasonably foreseeable use is to process, forward, or manage network traffic between devices, network segments, or between public and private networks.

NOTE 2: Unmanaged products with fixed functionality and no configuration interface are excluded from scope, as they lack the interfaces needed to implement the security controls of the present document.

The present document does not specify protocol conformance requirements, performance specifications, QoS metrics, or interoperability testing. Security controls for protocol implementation and vulnerability management remain within scope.

NOTE 3: Products that integrate particular wireless or wired communication technologies, such as Wi-Fi®, cellular, DECT, and DECT-2020 NR remain within scope when they function as routers, modems intended for connection to the internet, or switches

Routers, modems intended for connection to the internet, and switches intended for use in the industrial Operational Technology (OT) domain are excluded from the scope of the present document, see prEN 50770-5 [i.14].

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](#) (version 2 - April 2025): "European Cybersecurity Certification Group Sub-group on Cryptography Agreed Cryptographic Mechanisms".
- [2] Canadian Centre for Cyber Security ITSP.40.062 (January 2025): "[Guidance on securely configuring network protocols \(ITSP.40.062\)](#)".
- [3] [ETSI TS 119 312](#): "Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites".
- [4] [ETSI TS 133 210](#): "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)".
- [5] Arm Limited: "[Arm CCA Security Model 1.0](#)" (DEN0096).
- [6] [IRTF RFC 8439](#): "ChaCha20 and Poly1305 for IETF Protocols".
- [7] [IETF RFC 4418](#): "UMAC: Message Authentication Code using Universal Hashing".
- [8] [IETF RFC 9106](#): "Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications".
- [9] [IETF RFC 7914](#): "The scrypt Password-Based Key Derivation Function".
- [10] [IETF RFC 5295](#): "Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)".
- [11] [IETF RFC 8410](#): "Algorithm Identifiers for Ed25519, Ed448, X25519, and X448 for Use in the Internet X.509 Public Key Infrastructure".
- [12] [IRTF RFC 8032](#): "Edwards-Curve Digital Signature Algorithm (EdDSA)".
- [13] [IETF RFC 8420](#): "Using the Edwards-Curve Digital Signature Algorithm (EdDSA) in the Internet Key Exchange Protocol Version 2 (IKEv2)".
- [14] [IETF RFC 8110](#): "Opportunistic Wireless Encryption".
- [15] Wi-Fi™ Alliance: "[Wi-Fi Easy Connect™ Specification](#)", version 3.0.
- [16] [IETF RFC 9000](#): "QUIC: A UDP-Based Multiplexed and Secure Transport".
- [17] [IETF RFC 3411](#): "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks".
- [18] [IETF RFC 3412](#): "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)".
- [19] [IETF RFC 8205](#): "BGPsec Protocol Specification".

- [20] [IETF RFC 5709](#): "OSPFv2 HMAC-SHA Cryptographic Authentication".
- [21] [IETF RFC 7166](#): "Supporting Authentication Trailer for OSPFv3".
- [22] [IETF RFC 5310](#): "IS-IS Generic Cryptographic Authentication".
- [23] [IETF RFC 5925](#): "The TCP Authentication Option".
- [24] [IETF RFC 8915](#): "Network Time Security for the Network Time Protocol".

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] [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.6] [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 (General Data Protection Regulation).
 - [i.7] Recommendation ITU-T Y.2011 (2004): "General principles and general reference model for Next Generation Networks".
 - [i.8] IETF RFC 7426 (2015): "Software-Defined Networking (SDN): Layers and Architecture Terminology".
 - [i.9] NIST SP 800-133 Rev. 2 (June 2020): "Recommendation for Cryptographic Key Generation".
 - [i.10] ISO/IEC/IEEE 24765:2017: "Systems and software engineering - Vocabulary".
 - [i.11] IEEE Std 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".

- [i.12] Broadband Forum TR-069 Issue 1 Amendment 6 Corrigendum 1 (June 2020): "CPE WAN Management Protocol".
- [i.13] Broadband Forum TR-369 Issue 1 Amendment 4 Corrigendum 1 (June 2025): "User Services Platform (USP)".
- [i.14] prEN 50770-5: "Security for Operational Technologies - Part 5: Security Profile for routers, modems intended for the connection to the internet, and switches" (produced by CEN CENELEC).

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

- [i.15] [ENISA European Vulnerability Database \(EUVD\)](#), established pursuant to Article 12(2) of Directive (EU) 2022/2555.
- [i.16] [ENISA Single Reporting Platform \(SRP\)](#), established for Regulation (EU) 2024/2847.
- [i.17] IEEE 802.3™-2022: "IEEE Standard for Ethernet".
- [i.18] USB Implementers Forum: "Universal Serial Bus Specification", Revision 2.0 (April 2000).
- [i.19] USB Implementers Forum: "Universal Serial Bus 3.2 Specification", Revision 1.1 (September 2022).
- [i.20] USB Implementers Forum: "USB4 Specification", Version 2.0 (October 2022).
- [i.21] ETSI TS 136 300: "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (3GPP TS 36.300 version 9.9.0 Release 9)".
- [i.22] ETSI TS 138 300: "5G; NR; NR and NG-RAN Overall description; Stage-2 (3GPP TS 38.300 version 19.2.0 Release 19)".
- [i.23] ETSI TS 103 636-1: "DECT-2020 New Radio (NR); Part 1: Overview".
- [i.24] [BSI TR-02102-1 \(Version 2026-01, 31 January 2026\)](#): "Cryptographic Mechanisms: Recommendations and Key Lengths".
- [i.25] [ANSSI, Référentiel Général de Sécurité \(RGS\)](#): "Guide des mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques" (Cryptographic Mechanisms – Rules and Recommendations regarding the Choice and Sizing of Cryptographic Mechanisms), section B.1, version 2.04, 01/01/2020.
- [i.26] NIST SP 800-131A Rev. 2 (March 2019): "Transitioning the Use of Cryptographic Algorithms and Key Lengths"..
- [i.27] [IEEE 802.1AE™-2018](#): "IEEE Standard for Local and Metropolitan Area Networks - Media Access Control (MAC) Security".
- [i.28] [IEEE 802.1AR™-2018](#): "IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity".
- [i.29] [IEEE 1588™-2019](#): "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems".
- [i.30] [BSI TR-02102-2 \(Version 2026-01\)](#): "Cryptographic Mechanisms: Recommendations and Key Lengths: Use of Transport Layer Security (TLS)".
- [i.31] [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.32] [BSI TR-02102-4 \(Version 2026-01\)](#): "Cryptographic Mechanisms: Recommendations and Key Lengths - Use of Secure Shell (SSH)".

- [i.33] [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:

access point: network function that provides a wireless local area network for other devices, allowing them to access device services or connect to private or public networks

NOTE: Access points can use various wireless technologies. In home routers, this function is implemented using IEEE 802.11 technologies.

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

NOTE: Cryptographic algorithms describe cryptographic protocols/schemes/constructors/atomic primitives such as TLS/Symmetric Entity Authentication Schemes/AES-128 as part of a CMAC/AES-256.

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

NOTE: As defined in ISO/IEC/IEEE 24765 [i.10], 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

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

NOTE 1: Firmware includes boot sequences, operating system components, network protocol implementations, and management interfaces.

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

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

network interface: physical interface that can be used to access the functionality of router, modem intended for connection to the internet, or switch via a network

private network: closed network within a home or an organization that is not directly accessible by the general public and is controlled by or on behalf of the user

product: router, modem intended for connection to the internet, or switch 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 finalization 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

public network: network that is accessible by the general public and is not controlled by a user

EXAMPLE: Mobile networks such as 5G, or the internet.

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

secure-by-default configuration: configuration of the product, in product factory default state, that satisfies the requirements set out in clause [5.4.1](#)

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: Source: NIST SP 800-133 Rev. 2 [i.9].

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

transport layer port: logical interface on OSI Layer 4 used to address applications on a host that take part in end-to-end information exchange

NOTE: A host can run many network applications behind a single IP address. The Transport Layer Port Number identifies each application separately.

Wi-Fi® network: wireless local area network implemented according to IEEE 802.11 [i.33]

NOTE: In residential environments, Wi-Fi® is commonly used as the primary method for devices to connect to the public network and access the internet.

3.2 Symbols

Void.