



**Cyber Security (CYBER);
CRA;
Cybersecurity requirements for Network Management systems**

get full document from standards.iteh.ai

ReferenceDEN/CYBER-EUS-009

KeywordsCRA, cybersecurity, network management

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	10
Foreword.....	10
Modal verbs terminology.....	11
Introduction	11
1 Scope	12
2 References	12
2.1 Normative references	12
2.2 Informative references.....	13
3 Definition of terms, symbols and abbreviations.....	14
3.1 Terms.....	14
3.2 Symbols.....	15
3.3 Abbreviations	15
4 Product context.....	17
4.0 Introduction	17
4.1 Product Functions.....	17
4.1.0 Introduction.....	17
4.1.1 Network functions management	17
4.1.2 Software defined network management.....	18
4.1.3 Ecosystem management.....	18
4.1.4 ICT device management	19
4.2 Product Architecture.....	19
4.2.0 Introduction.....	19
4.2.1 Network architecture.....	20
4.2.1.1 Software Defined Network	21
4.2.1.2 Application in a SDN	22
4.2.1.3 Pocket deployment.....	22
4.2.1.4 Devices using provided connectivity	23
4.2.2 Controller design	23
4.2.3 Applying encryption in IETF RFC 1122	24
4.2.4 Inventory, device and subjects management.....	24
4.2.4.1 Identifying privileged subjects	24
4.2.4.2 Device management	24
4.2.4.3 Inventory management.....	25
4.3 Operational Environment	25
4.3.1 General description	25
4.3.2 Physical/Hardware environment	25
4.3.3 Logical/Software environment.....	26
4.3.4 Connectivity aspects	27
4.3.4.0 Introduction.....	27
4.3.4.1 Identity management.....	27
4.3.4.2 Attribute-Based Access Control.....	27
4.3.4.3 Role based authorisation	28
4.3.4.4 Trust initialisation	28
4.3.4.5 Risk management.....	28
4.4 Distribution of Security Functions	29
4.4.0 Introduction.....	29
4.4.1 Ancillary functionality.....	29
4.4.2 Related core functionalities.....	29
4.4.3 Security functions provided to other products	30
4.5 Users.....	30
4.6 Use Cases	30
4.6.0 Introduction.....	30
4.6.1 UC-1-HOME: Home NMS	31
4.6.2 UC-2-ENTER-*: Enterprise network.....	32

4.6.3	UC-3-TELCO: Telecommunications network.....	34
4.6.4	UC-4-SDN: Logical network deployment without physical hardware	35
4.6.5	UC-5-HYBRID: Physical network deployment with RDPS.....	36
4.6.6	UC-6-IOT: IoT network with monitoring data collection.....	39
4.6.7	UC-7-ICT: ICT Network Elements	40
4.6.8	UC-8-FLEET: Fleet management.....	42
4.6.9	UC-9-RESEARCH: Research NMS	43
4.6.10	UC-10-AIRGAP: Airgapped secure facility	43
4.6.11	UC-11-WATER: Management of distributed infrastructure	44
5	Technical requirements for products	44
5.1	Introduction - Applicability of the requirements	44
5.2	Appropriate level of cybersecurity	46
5.3	No known exploitable vulnerabilities.....	47
5.4	Secure by default configuration.....	47
5.5	Security updates	48
5.6	Authentication and access control	49
5.7	Confidentiality protection.....	50
5.8	Integrity protection	51
5.9	Data minimisation	51
5.10	Availability protection.....	52
5.11	Non-interference.....	52
5.12	Attack surface minimisation.....	53
5.13	Exploit mitigation.....	53
5.14	Monitoring.....	54
5.15	Factory reset and data portability	56
6	Assessment criteria for compliance with technical requirements	56
6.1	Introduction to the assessment and compliance criteria	56
6.1.0	Assessment guide.....	56
6.2	Appropriate level of cybersecurity	58
6.2.1	CYB_GENERAL-1	58
6.2.2	CYB_GENERAL-2	58
6.2.3	CYB_GENERAL-3	59
6.2.4	CYB_GENERAL-4	59
6.2.5	CYB_GENERAL-5	60
6.2.6	CYB_GENERAL-6	60
6.2.7	CYB_GENERAL-7	61
6.2.8	CYB_OPS-8	61
6.2.9	CYB_OPS-9	62
6.2.10	CYB_OPS-10	62
6.3	No known exploitable vulnerabilities.....	62
6.3.1	KEV_EXPLOIT-1	62
6.4	Secure by default configuration.....	64
6.4.1	SBD_TECH-1.....	64
6.4.2	SBD_TECH-2.....	64
6.4.3	SBD_TECH-3.....	65
6.5	Security updates	65
6.5.1	SU_UPDATES-1	65
6.5.2	SU_UPDATES-2	66
6.5.3	SU_UPDATES-3	66
6.5.4	SU_UPDATES-4	67
6.5.5	SU_UPDATES-5	67
6.5.6	SU_UPDATES-6	68
6.5.7	SU_UPDATES-7	68
6.5.8	SU_UPDATES-8	69
6.5.9	SU_UPDATES-9	69
6.5.10	SU_UPDATES-10	70
6.5.11	SU_UPDATES-11	70
6.5.12	SU_UPDATES-12	71
6.5.13	SU_UPDATES-13	71
6.5.14	SU_UPDATES-14	72

6.5.15	SU_UPDATES-15	72
6.6	Authentication and access control	73
6.6.1	AAC_AUTH-1	73
6.6.2	AAC_AUTH-2	73
6.6.3	AAC_AUTH-3	74
6.6.4	AAC_AUTH-4	74
6.6.5	AAC_AUTH-5	75
6.6.6	AAC_AUTH-6	76
6.6.7	AAC_AUTH-7	76
6.6.8	AAC_AUTH-8	77
6.6.9	AAC_AUTH-9	77
6.6.10	AAC_AUTH-10	78
6.6.11	AAC_AUTH-11	78
6.6.12	AAC_AUTH-12	79
6.6.13	AAC_MACHINE-13	80
6.6.14	AAC_MACHINE-14	80
6.7	Confidentiality protection	81
6.7.1	CON_INGEST-1	81
6.7.2	CON_INGEST-2	81
6.7.3	CON_CRYPT-3	82
6.7.4	CON_CHANNEL-4	82
6.7.5	CON_CHANNEL-5	83
6.8	Integrity protection	83
6.8.1	INT_CONF-1	83
6.8.2	INT_CONF-2	84
6.8.3	INT_CONF-3	84
6.8.4	INT_ROTATE-4	85
6.8.5	INT_ROTATE-5	85
6.8.6	INT_ROTATE-6	86
6.9	Data minimisation	86
6.9.1	DM_RETENTION-1	86
6.9.2	DM_RETENTION-2	87
6.9.3	DM_RETENTION-3	87
6.10	Availability protection	88
6.10.1	AP_HA-1	88
6.10.2	AP_HA-2	88
6.10.3	AP_HA-3	89
6.10.4	AP_HA-4	89
6.10.5	AP_HA-5	90
6.10.6	AP_HA-6	90
6.10.7	AP_HA-7	91
6.11	Non-interference	92
6.11.1	IM_SEGMENT-1	92
6.11.2	IM_SEGMENT-2	92
6.11.3	IM_SEGMENT-3	93
6.12	Attack surface minimisation	94
6.12.1	MAS_TECH-1	94
6.12.2	MAS_TECH-2	94
6.13	Exploit mitigation	95
6.13.1	EMM_ROUTE-1	95
6.13.2	EMM_ROUTE-2	95
6.13.3	EMM_ROUTE-3	96
6.14	Monitoring	96
6.14.0	Logging tests	96
6.14.1	MON_LOG-1	96
6.14.2	MON_LOG-2	97
6.14.3	MON_LOG-3	97
6.14.4	MON_LOG-4	98
6.14.5	MON_LOG-5	98
6.14.6	MON_LOG-6	99
6.14.7	MON_LOG-7	100
6.14.8	MON_LOG-8	100

6.14.9	MON_LOG-9	101
6.14.10	MON_LOG-10	101
6.14.11	MON_LOG-11	102
6.14.12	MON_LOG-12	102
6.14.13	MON_LOG-13	103
6.14.14	MON_METRICS-14	103
6.14.15	MON_METRICS-15	103
6.14.16	MON_METRICS-16	104
6.14.17	MON_METRICS-17	104
6.15	Factory reset and data portability	106
6.15.1	DRT_DELETE-1	106
6.15.2	DRT_DELETE-2	107

Annex A (informative):	Relationship between the present document and the essential cybersecurity requirements of EU Regulation (EU) 2024/2847	108
-------------------------------	---	------------

Annex B (informative):	Security analysis.....	112
-------------------------------	-------------------------------	------------

B.0	Overview	112
B.1	Assets	112
B.1.1	Data	112
B.1.2	Hardware	113
B.1.3	Product and managed element functions	113
B.2	Risk factors.....	113
B.2.1	Overview	113
B.2.2	RF-ACC_ASSETS: Accessibility of network connected to product assets	113
B.2.3	RF-COMPLEX_CONF: Complexity of network configuration.....	113
B.2.4	RF-COMPLEX_FUN: Complexity of product functions.....	114
B.2.5	RF-SENS_ASSETS: Sensitivity of managed assets.....	114
B.2.6	RF-SENS_FUN: Sensitivity of functions of product	114
B.2.7	RF-NUM: Number of managed elements	115
B.2.8	RF-ADMIN: Availability and skill of administration	115
B.3	Assumptions	115
B.4	Mapping of risk factors to use cases	115
B.4.1	UC-1-HOME security analysis.....	116
B.4.2	UC-2-ENTER security analysis	116
B.4.3	UC-3-TELCO security analysis	117
B.4.4	UC-4-SDN security analysis	117
B.4.5	UC-5-HYBRID security analysis	117
B.4.6	UC-6-IOT security analysis.....	117
B.4.7	UC-7-ICT security analysis.....	118
B.4.8	UC-8-FLEET security analysis	119
B.4.9	UC-9-RESEARCH security analysis	119
B.4.10	UC-10-AIRGAP security analysis	119
B.4.11	UC-11-WATER security analysis	119
B.5	Threats and security analysis of threats.....	119
B.5.1	Security analysis methodology.....	119
B.5.2	List of threats, risk assessments, and mitigations	120
B.5.2.0	Introduction.....	120
B.5.2.1	TH-UEVU: Unknown exploitable vulnerabilities	120
B.5.2.2	TH-KEVU: Known exploitable vulnerabilities	121
B.5.2.3	TH-CACC: Circumvention of access control	123
B.5.2.4	TH-DSTP: Unauthorised access to data stored.....	124
B.5.2.5	TH-UADT: Unauthorised access to data transmitted	125
B.5.2.6	TH-CONF: Access to assets via configuration errors.....	126
B.5.2.7	TH-AVAI: Denial of service attack on product.....	127
B.5.2.8	TH-DDoS: Interference with other devices	129

Annex C (informative):	Relationship between the present document and any related ETSI standards	131
Annexes D to F: Void.....		132
Annex G (informative):	Guidelines on the implementation of the present document.....	133
G.0	Guidance on use-cases.....	133
G.1	Guidance on no known exploitable vulnerabilities requirements.....	133
G.2	Guidance on secure by default configuration requirements	133
G.3	Guidance on authentication and access control requirements	134
G.4	Guidance on confidentiality protection requirements.....	134
G.5	Guidance on integrity protection requirements	135
G.6	Guidance on availability protection requirements.....	135
G.7	Guidance on non-interference requirements.....	135
G.8	Guidance on exploit mitigation requirements	136
G.9	Guidance on exploit mitigation requirements	136
G.10	Guidance on monitoring requirements	136
Annexes H to J: Void.....		137
Annex K (normative):	Generic cryptographic requirements and assessment.....	138
K.1	Cryptography.....	138
K.1.1	Requirement	138
K.1.2	Assessment of product cryptographic configuration	139
K.1.2.0	General.....	139
K.1.2.1	Assessment of ACM-listed cryptographic mechanisms.....	139
K.1.2.1.1	Assessment objective	139
K.1.2.1.2	Assessment preparation.....	139
K.1.2.1.3	Assessment activities	139
K.1.2.1.4	Assessment evidence.....	140
K.1.2.1.5	Assessment verdict.....	140
K.1.2.2	Assessment of ACM-extended cryptographic mechanisms.....	140
K.1.2.2.1	Assessment objective	140
K.1.2.2.2	Assessment preparation.....	140
K.1.2.2.3	Assessment activities	140
K.1.2.2.4	Assessment evidence.....	141
K.1.2.2.5	Assessment verdict.....	141
K.1.2.3	Assessment of interoperability-based cryptographic mechanisms.....	141
K.1.2.3.1	Assessment objective	141
K.1.2.3.2	Assessment preparation.....	141
K.1.2.3.3	Assessment activities	141
K.1.2.3.4	Assessment evidence.....	142
K.1.2.3.5	Assessment verdict.....	142
K.2	Crypto agility.....	142
K.2.1	Requirement	142
K.2.2	Assessment of crypto-agility	143
K.2.2.1	Assessment objective.....	143
K.2.2.2	Assessment preparation	143
K.2.2.3	Assessment activities	144
K.2.2.4	Assessment evidence	144
K.2.2.5	Assessment verdict	144
K.3	ACM-extended cryptographic mechanisms	144
K.3.1	Requirement	144
K.3.2	List of ACM-extended cryptographic mechanisms.....	144
K.3.3	Assessment.....	145
K.4	Interoperability-based cryptographic mechanisms.....	145
K.4.1	Requirement	145
K.4.2	List of interoperability-based cryptographic mechanisms.....	145
K.4.3	Assessment.....	145

Annexes L to Q: Void	146
Annex R (normative): Additional provisions for products relying on Remote Data Processing Solutions (RDPS)	147
R.1 Scope & Applicability	147
R.2 RDPS as a product-boundary extension.....	147
R.3 Threat Model	148
R.3.1 Introduction	148
R.3.2 Assets	148
R.3.3 Threat catalogue	149
R.3.3.1 Overview	149
R.3.3.2 T-RDPS-01 Loss of data authenticity of interactions across the RDPS boundary.....	149
R.3.3.3 T-RDPS-02 Loss of integrity of interactions across the RDPS boundary	149
R.3.3.4 T-RDPS-03 Unauthorised disclosure of interactions across the RDPS boundary	150
R.3.3.5 T-RDPS-04 Unavailability, unacceptable delay, or intolerable degradation of interactions across the RDPS boundary	150
R.3.4 Assets to Threats mapping	150
R.4 Security Requirements	150
R.4.1 Applicability of annex R requirements.....	150
R.4.2 Local product side requirements	151
R.4.2.1 REQ-RDPS-L-AUTH Data authenticity of interactions received from the RDPS side.....	151
R.4.2.2 REQ-RDPS-L-INTEG Integrity of interactions received from the RDPS side	151
R.4.2.3 REQ-RDPS-L-CONF Confidentiality of data exchanged with the RDPS side	151
R.4.2.4 REQ-RDPS-L-AVAIL Availability.....	152
R.4.3 RDPS side requirements.....	152
R.4.3.1 REQ-RDPS-R-AUTH Data authenticity of interactions received from the local product side	152
R.4.3.2 REQ-RDPS-R-INTEG Integrity of interactions received from the local product side	152
R.4.3.3 REQ-RDPS-R-CONF Confidentiality of data exchanged with the local product side	152
R.4.3.4 REQ-RDPS-R-AVAIL Availability	153
R.4.4 Threats ↔ Requirements mapping.....	153
R.5 Conformity assessment.....	153
R.5.1 Overview	153
R.5.2 Local product side assessments	153
R.5.2.1 REQ-RDPS-L-AUTH assessment	153
R.5.2.1.1 Objective	153
R.5.2.1.2 Preparation	153
R.5.2.1.3 Activities	154
R.5.2.1.4 Verdict.....	154
R.5.2.1.5 Evidence.....	154
R.5.2.2 REQ-RDPS-L-INTEG assessment	154
R.5.2.2.1 Objective	154
R.5.2.2.2 Preparation	154
R.5.2.2.3 Activities	155
R.5.2.2.4 Verdict.....	155
R.5.2.2.5 Evidence.....	155
R.5.2.3 REQ-RDPS-L-CONF assessment.....	155
R.5.2.3.1 Objective	155
R.5.2.3.2 Preparation	155
R.5.2.3.3 Activities	155
R.5.2.3.4 Verdict.....	156
R.5.2.3.5 Evidence.....	156
R.5.2.4 REQ-RDPS-L-AVAIL assessment.....	156
R.5.2.4.1 Objective	156
R.5.2.4.2 Preparation	156
R.5.2.4.3 Activities	156
R.5.2.4.4 Verdict.....	157
R.5.2.4.5 Evidence.....	157
R.5.3 RDPS side assessments	157

R.5.3.1	REQ-RDPS-R-AUTH assessment	157
R.5.3.1.1	Objective	157
R.5.3.1.2	Preparation	157
R.5.3.1.3	Activities	157
R.5.3.1.4	Verdict.....	158
R.5.3.1.5	Evidence.....	158
R.5.3.2	REQ-RDPS-R-INTEG assessment	158
R.5.3.2.1	Objective	158
R.5.3.2.2	Preparation	158
R.5.3.2.3	Activities	158
R.5.3.2.4	Verdict.....	159
R.5.3.2.5	Evidence.....	159
R.5.3.3	REQ-RDPS-R-CONF assessment	159
R.5.3.3.1	Objective	159
R.5.3.3.2	Preparation	159
R.5.3.3.3	Activities	159
R.5.3.3.4	Verdict.....	159
R.5.3.3.5	Evidence.....	160
R.5.3.4	REQ-RDPS-R-AVAIL assessment.....	160
R.5.3.4.1	Objective	160
R.5.3.4.2	Preparation	160
R.5.3.4.3	Activities	160
R.5.3.4.4	Verdict.....	160
R.5.3.4.5	Evidence.....	161
Annex S (informative):	Change history	162
History		163

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.

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) 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 defines cybersecurity requirements for products with digital elements (product) whose intended purpose is to manage connected network elements, such as servers, routers, switches, workstations, printers or mobile devices, by monitoring them and controlling their network operations and configuration. The present document is part of a broader group of vertical standards developed to support the Cyber Resilience Act (CRA) [i.1] and should not be considered a standalone resource. Users are expected to consult it in conjunction with the CRA itself [i.1], the associated legal guidance [i.20], as well as relevant horizontal and neighbouring vertical standards cited in clause 2, such as prEN 40000-1-1 [i.4], prEN 40000-1-2 [i.5], prEN 40000-1-3 [i.6], and prEN 40000-1-4 [i.7]. Material already addressed in those sources is not repeated in the present document.

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 C informs the possible relationship between the product in the present document and other possible vertical products and their corresponding CRA-related harmonised standards.

Annex G presents further information on guidance for the application of the present document.

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

Annex R provides supplementary requirements and assessment provisions where a product relies on Remote Data Processing Solutions (RDPS) for the provision or support of one or more product functions.

1 Scope

The present document specifies technical requirements and corresponding assessment criteria for Network Management Systems related to cybersecurity. The products with digital elements in scope, thereafter "NMS":

- are specified within the "technical description" of the "category of product" number "6" by the Commission Implementing Regulation (EU) 2025/2392 [i.2] as: "Products with digital elements that manage connected network elements, such as servers, routers, switches, workstations, printers or mobile devices, by monitoring them and controlling their network operations and configuration".

This category includes but is not limited to end-to-end management systems and dedicated configuration management systems, such as controllers for software-defined networking.

- The products with digital elements in scope are only covered within the product context described in clause 4 of the present document.

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.

This includes, but is not limited to, Mobile Device Management systems and Software Defined Networking, e.g when an SDN-controller is a stand-alone product using a network management protocol as its South Bound Interface (SBI).

NMS intended for use in the industrial Operational Technology (OT) [i.18] domain are excluded from the scope of the present document.

An NMS is a product controlling at least partially connected devices with network access. Despite its central positioning, an NMS can be an aggregate of several components, including but not limited to: end-to-end management systems, dedicated configuration management systems, or controllers for software-defined networking.

NMS can be composed of several components or can implement additional functions that are outside the scope of the present document.

EXAMPLE: Aggregate product design would be an implementation where the operating system acts as an abstraction layer for the system(s) that host the NMS, or the networking interfaces.

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" [ACM].
- [2] [IETF RFC 1122 \(October 1989\)](#): "Requirements for Internet Hosts - Communication Layers".

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] prEN 40000-1-2: "Cybersecurity requirements for products with digital elements – Part 1-2: Principles, product risk management, and lifecycle activities"(produced by CEN CENELEC).
- NOTE: Version and date to be added upon its publication by CEN CENELEC.
- [i.6] prEN 40000-1-3: "Cybersecurity requirements for products with digital elements – Part 1-3: Vulnerability handling"(produced by CEN CENELEC).
- NOTE: Version and date to be added upon its publication by CEN CENELEC.
- [i.7] prEN 40000-1-4: "Cybersecurity requirements for products with digital elements – Part 1-4: Security controls – Generic security requirements"(produced by CEN CENELEC).
- NOTE: Version and date to be added upon its publication by CEN CENELEC.
- [i.8] IETF RFC 1918 (February 1996): "BCP 5: Address Allocation for Private Internets".
 - [i.9] NIST SP 800-63B-4: "Authentication & Authenticator Management".
 - [i.10] ISO/IEC 27000:2026: "Information technology — Security techniques — Information security management systems — Overview and vocabulary".
 - [i.11] ETSI EN 304 624 (V1.1.1): "Cyber Security (CYBER); CRA; Cybersecurity requirements for Public key infrastructure and digital certificate issuance software".
 - [i.12] ETSI EN 304 620 (V1.1.1): " Cyber Security (CYBER); CRA; Cybersecurity requirements for Virtual Private Networks (VPNs)".

- [i.13] [CEN/CLC EN 50770-4](#): "Security for Operational Technologies - Part 4: Security Profile for products with digital elements with the function of virtual private network (VPN)" (produced by CEN CENELEC).
- [i.14] ETSI EN 304 622 (V1.1.1): "Cyber Security (CYBER); CRA; Cybersecurity requirements for Security information and event management (SIEM) systems".
- [i.15] ETSI EN 304 626 (V1.1.1): "Cyber Security (CYBER); CRA; Cybersecurity requirements for operating systems".
- [i.16] ETSI EN 304 627 (V1.1.1): "Cyber Security (CYBER); CRA; Cybersecurity requirements for routers, modems intended for the connection to the internet, and switches".
- [i.17] ETSI EN 304 642 (V1.1.1): "CYBER; CRA; Cybersecurity Requirements for Network Functions of Telecommunications Systems".
- [i.18] Example source for [DDoS related threat reports](#).
- [i.19] prEN 50770 series: "Security for operational technologies" (produced by CENELEC).
- [i.20] EC: "[Commission CRA draft legal guidance](#)".
- [i.21] BSI Technical Guideline TR-02102-1 (2026-01): "Cryptographic Mechanisms: Recommendations and Key Lengths".
- [i.22] BSI Technical Guideline TR-02102-2 (2026-01): "Cryptographic Mechanisms: Recommendations and Key Lengths: Use of Transport Layer Security (TLS)".
- [i.23] BSI Technical Guideline TR-02102-3 (2026-01): "Cryptographic Mechanisms: Recommendations and Key Lengths – Use of Internet Protocol Security (IPsec) and Internet Key Exchange (IKEv2)".
- [i.24] BSI Technical Guideline TR-02102-4 (2026-01): "Cryptographic Mechanisms: Recommendations and Key Lengths – Use of Secure Shell (SSH)".

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:

component: software or hardware intended for integration into an electronic information system

cryptographic mechanism: security-related procedure using cryptography

cryptographic property: property provided or supported by a cryptographic mechanism

NOTE 1: The term "cryptographic mechanism" is used in the present document as an umbrella term covering the categories used in the ECCG Agreed Cryptographic Mechanisms (ACM) catalogue [1], including cryptographic algorithms, primitives, schemes, protocols, protocol profiles, cipher suites, modes of operation, constructions and parameter sets.

NOTE 2: The terms "cryptographic primitive", "cryptographic construction", "cryptographic scheme" and "cryptographic protocol" are used consistently with the ECCG Agreed Cryptographic Mechanisms (ACM) catalogue [1].

NOTE 3: A cryptographic mechanism can be specified at different levels of abstraction. For example, AES is a cryptographic primitive, AES-GCM is a mode of operation / authenticated encryption construction, TLS 1.3 is a protocol, a TLS 1.3 restricted cipher-suite profile is a protocol profile, and TLS_AES_128_GCM_SHA256 is a cipher suite.

NOTE 4: Cryptographic properties include, for example, confidentiality, integrity, authenticity, entity authentication, message authentication, key establishment, key confirmation, replay protection, collision resistance, second-preimage resistance, pre-image resistance, signature unforgeability, non-repudiation, forward secrecy and password-verifier protection. Where relevant, a cryptographic property can be expressed using a formal cryptographic notion, for example IND-CPA, IND-CCA, IND-CCA2, EUF-CMA, SUF-CMA or authenticated key exchange security.

NOTE 5: A cryptographic property is distinct from a product-level technical requirement, although it can support such a requirement. For example, a secure communication requirement can rely on cryptographic properties such as confidentiality, integrity and authentication.

forward proxy server: proxy server with intelligent web-caching and improvements of accelerating data transmissions combined with access controls

log: record of an operational event

machine user: virtual user used to access the system programming interfaces

managed element: physical or virtual device managed by the product

product user: consumers or customers or entities like companies and institutions that operate the product in its intended and foreseeable use case

secure channel: cryptographically protected communication channel

subject: system user, machine user, or a process being authenticated by the identity provider

system user: person having the credentials to login to the product to operate administrative actions to control and maintain the managed element

trace: record of a system status with all relevant data that can be gathered

3.2 Symbols

Void.

3.3 Abbreviations

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

ABAC	Attribute-Based Access Control
ACL	Access Control Lists
ACM	Agreed Cryptographic Mechanisms
ACN	Agenzia per la Cybersicurezza Nazionale

NOTE: In English: National Cybersecurity Agency of Italy.

AES	Advanced Encryption Standard
AES-GCM	Advanced Encryption Standard - Galois/Counter Mode
AES-XTS	Advanced Encryption Standard in XEX-based Tweaked Codebook mode with Ciphertext Stealing
API	Application Programming Interface
ARP	Address Resolution Protocol
AVAI	Availability
C2SP	Community Cryptography Specification Project
CA	Certificate Authority
CACC	Circumvention of Access Control
CISA	Cybersecurity and Infrastructure Security Agency
CONF	Confidentiality
CPU	Central Processing Unit
CRA	Cyber Resilience Act
CSP	Communication System Provider
CVE	Common Vulnerabilities and Exposures
DA	Data Asset