



**Cyber Security (CYBER);
CRA;
Cybersecurity requirements for software that searches for,
removes, or quarantines malicious software**

get full document from standards.iteh.ai

Reference

DEN/CYBER-EUS-0018

Keywords

antimalware, antivirus, CRA, cybersecurity,
security analysis, security profiles,
security requirements, threat analysis, use cases

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.....	8
Modal verbs terminology.....	9
Introduction	9
1 Scope	10
2 References	10
2.1 Normative references	10
2.2 Informative references.....	11
3 Definition of terms, symbols and abbreviations.....	12
3.1 Terms.....	12
3.2 Symbols.....	13
3.3 Abbreviations	13
4 Product context.....	16
4.0 Introduction	16
4.1 Product Functions.....	16
4.2 Product Architecture.....	16
4.3 Operational Environment	17
4.3.1 General description.....	17
4.3.2 Physical/Hardware environment.....	18
4.3.3 Logical/Software environment.....	18
4.3.4 Connectivity aspects	19
4.4 Distribution of Security Functions	20
4.4.1 Cybersecurity Functionalities Offered to Other Products	20
4.4.2 Cybersecurity Functionalities Required from Other Products	20
4.5 Users.....	20
4.6 Use Cases	21
4.6.1 Introduction.....	21
4.6.2 UC1: Limited Operational Context.....	21
4.6.3 UC2: Baseline Operational Context.....	22
4.6.4 UC3: Elevated Operational Context	22
4.6.5 UC4: High Value Operational Context	22
4.6.6 UC5: Critical Operational Context	22
4.6.7 Use cases to risk factors and risk levels mapping	22
5 Technical requirements for products	23
5.1 Introduction - Applicability of the requirements	23
5.2 Appropriate level of cybersecurity	23
5.3 No known exploitable vulnerabilities.....	23
5.4 Secure by default configuration.....	24
5.5 Security updates	24
5.6 Authentication and access control	26
5.7 Confidentiality protection.....	27
5.8 Integrity protection.....	28
5.9 Data minimisation	28
5.10 Availability protection.....	28
5.11 Non-interference.....	29
5.12 Attack surface minimisation.....	30
5.13 Exploit mitigation.....	30
5.14 Monitoring.....	31
5.15 Factory reset and data portability	31
6 Assessment criteria for compliance with technical requirements	32
6.1 Introduction to the assessment and compliance criteria	32
6.1.0 Assessment guide.....	32

6.1.1	Inability to comply with assessment methodology	33
6.2	Appropriate level of cybersecurity	34
6.3	No known exploitable vulnerabilities.....	34
6.3.1	REQ-KEV-01	34
6.4	Secure by default configuration.....	36
6.4.1	REQ-SBD-01	36
6.4.2	REQ-SBD-02	38
6.4.3	REQ-SBD-03	39
6.4.4	REQ-SBD-04	41
6.4.5	REQ-SBD-05	43
6.5	Security updates	43
6.5.1	REQ-SU-01.....	43
6.5.2	REQ-SU-02.....	45
6.5.3	REQ-SU-03.....	48
6.5.4	REQ-SU-04.....	49
6.5.5	REQ-SU-05.....	52
6.5.6	REQ-SU-06.....	54
6.5.7	REQ-SU-07.....	56
6.5.8	REQ-SU-08.....	58
6.5.9	REQ-SU-09.....	60
6.6	Authentication and access control	61
6.6.1	REQ-AAC-01	61
6.6.2	REQ-AAC-02	63
6.6.3	REQ-AAC-03	65
6.6.4	REQ-AAC-04	66
6.6.5	REQ-AAC-05	68
6.6.6	REQ-AAC-06	70
6.6.7	REQ-AAC-07	71
6.6.8	REQ-AAC-08	73
6.6.9	REQ-AAC-09	75
6.6.10	REQ-AAC-10	76
6.6.11	REQ-AAC-11	78
6.7	Confidentiality protection.....	80
6.7.1	REQ-CON-01	80
6.7.2	REQ-CON-02	82
6.7.3	REQ-CON-03	85
6.7.4	REQ-CON-04	87
6.8	Integrity protection	88
6.8.1	REQ-INT-01	88
6.8.2	REQ-INT-02	90
6.9	Data minimisation	92
6.9.1	REQ-DM-01	92
6.10	Availability protection.....	93
6.10.1	REQ-AP-01.....	93
6.10.2	REQ-AP-02.....	95
6.10.3	REQ-AP-03.....	97
6.10.4	REQ-AP-04.....	98
6.11	Non-interference.....	101
6.11.1	REQ-NI-01	101
6.11.2	REQ-NI-02	102
6.12	Attack surface minimisation.....	104
6.12.1	REQ-ASM-01	104
6.12.2	REQ-ASM-02	106
6.12.3	REQ-ASM-03	107
6.13	Exploit mitigation.....	109
6.13.1	REQ-EM-01.....	109
6.13.2	REQ-EM-02.....	111
6.14	Monitoring.....	112
6.14.1	REQ-MON-01	112
6.14.2	REQ-MON-02	114
6.14.3	REQ-MON-03	116
6.14.4	REQ-MON-04	117

6.14.5	REQ-MON-05	119
6.14.6	REQ-MON-06	121
6.15	Factory reset and data portability	122
6.15.1	REQ-FRD-01	122
6.15.2	REQ-FRD-02	124

Annex A (informative):	Relationship between the present document and the essential cybersecurity requirements of EU Regulation (EU) 2024/2847	126
-------------------------------	---	------------

Annex B (informative):	Security analysis.....	130
-------------------------------	-------------------------------	------------

B.0	Introduction	130
-----	--------------------	-----

B.1	Threats and Risk Factors Landscape	130
-----	--	-----

B.1.1	Threats.....	130
-------	--------------	-----

B.1.1.1	Introduction.....	130
---------	-------------------	-----

B.1.1.2	TH1 - Threats related to Updates and Signatures	130
---------	---	-----

B.1.1.3	TH2 - Threats to Core Components and Self-Protection	130
---------	--	-----

B.1.1.4	TH3 - Threats to Communication and Data Exchange	131
---------	--	-----

B.1.1.5	TH4 - Supply Chain and Third-Party Component Threats	131
---------	--	-----

B.1.1.6	TH5 - Advanced Threat Actor Techniques.....	131
---------	---	-----

B.1.1.7	TH6 - User-Facing Threats	131
---------	---------------------------------	-----

B.1.2	Risks Factors	132
-------	---------------------	-----

B.1.2.1	Introduction.....	132
---------	-------------------	-----

B.1.2.2	Likelihood-related Risk Factors.....	132
---------	--------------------------------------	-----

B.1.2.3	Magnitude-related Risk Factors.....	133
---------	-------------------------------------	-----

B.1.3	Threat justification and mitigation	134
-------	---	-----

B.2	Security Profiles	135
-----	-------------------------	-----

B.2.1	General	135
-------	---------------	-----

B.2.2	Minimal Cybersecurity.....	135
-------	----------------------------	-----

B.2.3	Medium Cybersecurity.....	136
-------	---------------------------	-----

B.2.4	High Cybersecurity.....	136
-------	-------------------------	-----

B.3	Information on the methodology for the security analysis of cybersecurity risks used to develop the present document.....	136
-----	---	-----

B.3.1	Principles and references.....	136
-------	--------------------------------	-----

B.3.2	Risk model.....	137
-------	-----------------	-----

B.3.3	Risk criteria	137
-------	---------------------	-----

B.3.3.1	Introduction.....	137
---------	-------------------	-----

B.3.3.2	Risk Likelihood (L)	137
---------	---------------------------	-----

B.3.3.3	Magnitude of loss or disruption (M).....	137
---------	--	-----

B.3.3.4	Qualitative risk matrix	138
---------	-------------------------------	-----

B.3.4	Process.....	138
-------	--------------	-----

B.3.5	Risk computation and mapping	138
-------	------------------------------------	-----

B.3.6	Example of Risk Analysis	139
-------	--------------------------------	-----

B.4	Use Cases Security Analysis	140
-----	-----------------------------------	-----

B.4.1	Introduction	140
-------	--------------------	-----

B.4.2	UC1: Limited Impact Context	140
-------	-----------------------------------	-----

B.4.3	UC2: Baseline Impact Context.....	141
-------	-----------------------------------	-----

B.4.4	UC3: Elevated Impact Context.....	142
-------	-----------------------------------	-----

B.4.5	UC4: High Impact Context.....	143
-------	-------------------------------	-----

B.4.6	UC5: Critical Impact Context.....	144
-------	-----------------------------------	-----

Annex C (informative):	Relationship between the present document and any related ETSI standards	146
-------------------------------	---	------------

Annexes D to F:	Void	147
------------------------	-------------------	------------

Annex G (informative):	Guidelines on the implementation of the present document.....	148
-------------------------------	--	------------

Annexes H to J:	Void	150
------------------------	-------------------	------------

Annex K (normative):	Generic cryptographic requirements and assessment.....	151
K.1	Cryptography.....	151
K.1.1	Requirement	151
K.1.2	Assessment of product cryptographic configuration	152
K.1.2.0	General.....	152
K.1.2.1	Assessment of ACM-listed cryptographic mechanisms.....	152
K.1.2.1.1	Assessment objective.....	152
K.1.2.1.2	Assessment preparation	152
K.1.2.1.3	Assessment activities	152
K.1.2.1.4	Assessment evidence	153
K.1.2.1.5	Assessment verdict	153
K.1.2.2	Assessment of ACM-extended cryptographic mechanisms.....	153
K.1.2.2.1	Assessment objective.....	153
K.1.2.2.2	Assessment preparation	153
K.1.2.2.3	Assessment activities	153
K.1.2.2.4	Assessment evidence	154
K.1.2.2.5	Assessment verdict	154
K.1.2.3	Assessment of interoperability-based cryptographic mechanisms.....	154
K.1.2.3.1	Assessment objective.....	154
K.1.2.3.2	Assessment preparation	154
K.1.2.3.3	Assessment activities	154
K.1.2.3.4	Assessment evidence	155
K.1.2.3.5	Assessment verdict	155
K.2	Crypto agility.....	155
K.2.1	Requirement	155
K.2.2	Assessment of crypto-agility	156
K.2.2.1	Assessment objective	156
K.2.2.2	Assessment preparation.....	156
K.2.2.3	Assessment activities	157
K.2.2.4	Assessment evidence.....	157
K.2.2.5	Assessment verdict.....	157
K.3	ACM-extended cryptographic mechanisms	157
K.3.1	Requirement	157
K.3.2	List of ACM-extended cryptographic mechanisms.....	157
K.3.3	Assessment.....	158
K.4	Interoperability-based cryptographic mechanisms.....	159
K.4.1	Requirement	159
K.4.2	List of interoperability-based cryptographic mechanisms.....	159
K.4.3	Assessment.....	159
Annexes L to Q:	Void	160
Annex R (normative):	Requirements on RDPS.....	161
R.0	Introduction	161
R.1	RDPS as a product-boundary extension.....	161
R.2	Threat Model	162
R.2.0	Introduction	162
R.2.1	Assets	162
R.2.2	Threat catalogue	163
R.2.3	Assets and Threats Mapping	164
R.3	Security Requirements	164
R.3.1	General	164
R.3.2	Applicability of Annex R requirements.....	164
R.3.3	Local product side requirements	165
R.3.3.1	Data authenticity of interactions received from the RDPS side.....	165
R.3.3.2	Integrity of interactions received from the RDPS side	166
R.3.3.3	Confidentiality of data exchanged with the RDPS side	166

R.3.3.4	Availability	167
R.3.4	RDPS side requirements.....	167
R.3.4.1	Data authenticity of interactions received from the local product side	167
R.3.4.2	Integrity of interactions received from the local product side.....	168
R.3.4.3	Confidentiality of data exchanged with the local product side	168
R.3.4.4	Availability	169
R.3.5	Mapping of Threats and Requirements	170
R.4	Conformity assessment.....	170
R.4.1	Local product side requirements	170
R.4.1.1	REQ-RDPS-L-AUTH-001.....	170
R.4.1.2	REQ-RDPS-L-AUTH-002.....	171
R.4.1.3	REQ-RDPS-L-AUTH-003.....	172
R.4.1.4	REQ-RDPS-L-INTEG-001.....	173
R.4.1.5	REQ-RDPS-L-INTEG-002.....	174
R.4.1.6	REQ-RDPS-L-INTEG-003.....	174
R.4.1.7	REQ-RDPS-L-CONF-001	175
R.4.1.8	REQ-RDPS-L-CONF-002	176
R.4.1.9	REQ-RDPS-L-CONF-003	177
R.4.1.10	REQ-RDPS-L-AVAIL-001	178
R.4.1.11	REQ-RDPS-L-AVAIL-002	179
R.4.1.12	REQ-RDPS-L-AVAIL-003	180
R.4.2	RDPS side requirements.....	181
R.4.2.1	REQ-RDPS-R-AUTH-001	181
R.4.2.2	REQ-RDPS-R-AUTH-002	182
R.4.2.3	REQ-RDPS-R-AUTH-003	183
R.4.2.4	REQ-RDPS-R-INTEG-001	184
R.4.2.5	REQ-RDPS-R-INTEG-002	184
R.4.2.6	REQ-RDPS-R-INTEG-003	185
R.4.2.7	REQ-RDPS-R-CONF-001.....	186
R.4.2.8	REQ-RDPS-R-CONF-002.....	187
R.4.2.9	REQ-RDPS-R-CONF-003.....	188
R.4.2.10	REQ-RDPS-R-AVAIL-001.....	189
R.4.2.11	REQ-RDPS-R-AVAIL-002.....	190
R.4.2.12	REQ-RDPS-R-AVAIL-003.....	190
Annex S (informative):	Change history	192
History		194

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) 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 defines cybersecurity requirements for products with digital elements (product) whose intended purpose is to search for, remove, or quarantine malicious software or code. These products are intended to protect a protected system against malicious software or code that can compromise its confidentiality, integrity, or availability.

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.13], 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 software products with digital elements that detect or search for malicious software or code on a device, or remove or quarantine such software or code to prevent or mitigate system infection related to cybersecurity. The products with digital elements in scope, thereafter "the product":

- are specified within the "technical description" of the "category of product" number "4" by the Commission Implementing Regulation (EU) 2025/2392 [i.2] as:
 - "Software products with digital elements, typically referred to as antivirus or antimalware, that detect or search for malicious software or code on devices, or remove or quarantine such software or code, in order to maintain the integrity, confidentiality, or availability of such devices.

In the context of this category of products, malicious software means software containing malicious features or capabilities that can cause harm directly or indirectly to the user and/or the computer system, such as viruses, worms, ransomware, spyware and trojans.

This category includes but is not limited to software that detects or searches for malicious software in real-time or manually, rootkit detection and rescue disks with the core functionality of searching, removing or quarantining malicious software."

- are only covered within the product context described in clause 4.

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

The present document specifies technical characteristics and methods of assessment for Antivirus/Antimalware products.

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] [IETF-IRTF RFC 7748](#) (Version 11 - January 2016): "Elliptic Curves for Security".
- [3] [IETF-IRTF RFC 8032](#) (Version 08 - January 2017): "Edwards-Curve Digital Signature Algorithm (EdDSA)".
- [4] [NIST FIPS 186-5](#) (Version 5 - February 2023): "Digital Signature Standard (DSS)".
- [5] [IETF-IRTF RFC 9106](#) (Version 14 - September 2021): "Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications".
- [6] [IETF RFC 7914](#) (Version 5 - August 2016): "The scrypt Password-Based Key Derivation Function".

- [7] [IETF-IRTF RFC 8439](#) (Version 4 - June 2018): "ChaCha20 and Poly1305 for IETF Protocols".

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] ETSI EN 304 626: "CYBER; CRA; Cybersecurity requirements for operating systems".
- NOTE: Version and date to be added upon its publication by ETSI.
- [i.9] ETSI EN 304 636: "Cyber Security (CYBER); CRA; Cybersecurity requirements for firewalls, intrusion detection and/or prevention systems".
- NOTE: Version and date to be added upon its publication by ETSI.
- [i.10] ETSI EN 304 622: "Cyber Security (CYBER); CRA; Cybersecurity requirements for Security information and event management (SIEM) systems".

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

- [i.11] ETSI EN 304 623: "Cyber Security (CYBER); CRA; Cybersecurity requirements for boot managers".

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

- [i.12] [Directive \(EU\) 2022/2555](#) of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). .
- [i.13] EC: "[Commission CRA draft legal guidance](#)".
- [i.14] ISO/IEC 27005: "Information cybersecurity, cybersecurity and privacy protection — Guidance on managing information cybersecurity risks".
- [i.15] [BSI TR-02102-1](#) (Version: 2026-01 - January 2026): "Cryptographic Mechanisms: Recommendations and Key Lengths".
- [i.16] [IETF-IRTF draft-irtf-cfrg-aegis-aead-18](#) (Version 18 - October 2025): "The AEGIS Family of Authenticated Encryption Algorithms".
- [i.17] Conference Paper (Version 1.1 - August 2013): "[AEGIS: A Fast Authenticate Encryption Algorithm](#)".

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:

antivirus/antimalware: software product whose essential function(s) is searching, detecting, removing, or quarantining malicious software or code

cryptographic item: cryptographic algorithm, primitive, scheme, protocol, protocol profile, cipher suite, mode of operation, construction or parameter set used to provide or support a cryptographic property

NOTE: A cryptographic item 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.

cryptographic mechanism: security-related procedure using cryptography

NOTE 1: The term "cryptographic mechanism" is used in Annex K 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 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.

cryptographic property: property provided or supported by a cryptographic mechanism

NOTE 1: 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 2: 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.

detection rules update: malware signatures, heuristic rules, detection database

heuristic analysis: detection method based on rule- or behaviour-based analysis used to identify potentially malicious software or code not matching known signatures

interoperability: need to support interoperability with identified systems, deployments or operational environments that require use of specific cryptographic items which may not comply with the state-of-the-art in the domain

known exploitable vulnerabilities: Exploitable vulnerability as defined in [i.1] Article 3 point (41) that it is known.

malware software (malware): software designed with malicious intent that can disrupt, damage, or gain unauthorised access

multi-factor authentication: cybersecurity process requiring users to provide two or more verification factors to gain access to an account or application

personal data: As defined in [i.1] Article 3 point (47).

principle of least privilege: every user, process, service, and component gets only the minimum access (permissions, data, time, and network reach) needed to do its job with the goal to shrink attack surface and limit blast radius if something is compromised

NOTE: This definition is given in prEN 40000-1-1 [i.4].

protected system: PwDE, system or environment on which the antivirus/antimalware

quarantine: isolation of suspected malicious software or code to prevent execution or interaction with the protected system

security update: software patch addressing a product vulnerability

signature-based detection: detection method based on comparison with known patterns or signatures of malicious software or code

update mechanism: process used to retrieve, verify, and apply updates to signatures, detection logic, or related cybersecurity components

virus: type of malware specifically designed to self-replicate by injecting its own code into other programs code files

3.2 Symbols

Void.

3.3 Abbreviations

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

3GPP	3 rd Generation Partnership Project
AAC	Authentication and Access Control
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
 ASLR Address Space Layout Randomization
 ASM Attack Surface Minimisation
 BSI Bundesamt für Sicherheit in der Informationstechnik

NOTE: In English: Federal Office for Information Security.

CAVP Cryptographic Algorithm Validation Program
 CEN Comité Européen de Normalisation

NOTE: In English: European Committee for Standardization.

CENELEC Comité Européen de Normalisation Électrotechnique

NOTE: In English: European Committee for Electrotechnical Standardization.

CERT Computer Emergency Response Team
 CFI Control Flow Integrity
 CI/CD Continuous Integration and Continuous Delivery/Deployment
 CIA Confidentiality, Integrity, Availability
 CISA Cybersecurity and Infrastructure Security Agency
 CLI Command Line Interface
 CMVP Cryptographic Module Validation Program
 CON CONFIDENTIAL
 CPU Central Processing Unit
 CRA Cyber Resilience Act
 CSA CyberSecurity Act
 CSRC Computer Security Resource Center
 CVE Common Vulnerabilities and Exposures
 DA Data Asset
 DB Database
 DEP/NX Data Execution Prevention/No-Execute
 DNS Domain Name Server
 DoS Denial of Service
 DPIA Data Privacy Impact Assessments
 EDR Endpoint Detection and Response
 ENISA European Union Agency for Cybersecurity

NOTE: Originally established as European Network and Information Security Agency.

EPC Energy Performance Certificate
 ETSI European Telecommunications Standards Institute
 EUF-CMA Existential Unforgeability under Adaptive Chosen Message Attack
 FRD Factory Reset and Data portability
 HKDF HMAC-based Key Derivation Function
 HMAC Hash-based Message Authentication Code
 HTTP Hypertext Transfer Protocol
 HTTPS Hypertext Transfer Protocol Secure
 I/O Input/Output
 IAM Identity and Access Management
 ID Identifier
 IDS Intrusion Detection System
 IEC International Electrotechnical Commission
 IEEE Institute of Electrical and Electronics Engineers
 IETF Internet Engineering Task Force
 IND-CCA Indistinguishability under adaptive Chosen-Ciphertext Attack
 IND-CPA Indistinguishability under Chosen-Plaintext Attack

INT	INTEgrity
IP	Internet Protocol
IPC	Inter-Process Communication
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
IT	Information Technology
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
JTC	Joint Technical Committee
KEV	Known Exploitable Vulnerability
LAN	Local Area Network
MAC	Media Access Control
MFA	Multi-Factor Authentication
MITM	Machine-In-The-Middle
MON	MONitoring
MTTD	Mean Time To Detect
MTTR	Mean Time To Respond
NIC	Network Interface Card
NIS2	Network and Information Security Directive 2
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OoA	Object of Assessment
O-RAN	Open Radio Access Network
OS	Operating System
PoLP	Principle of Least Privilege
PwDE	Product with Digital Elements
RBAC	Role-Based Access Control
RDPS	Remote Data Processing Solution
RF	Risk Factor
RFL	Risk Factor on Likelihood
RFM	Risk Factor on Magnitude
RTO	Recovery Time Objective
SaaS	Security as a Service
SBD	Secure By Default SBOM
SDK	Software Development Kit
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOAR	Security Orchestration Automation and Response
SOG-IS	Senior Officials Group - Information Systems Security
SP	Security Profile
SPDX	Software Package Data eXchange
SU	Security Updates
SUF-CMA	Strong Existential Unforgeability under Chosen-Message Attack
TC	Technical Committee
TCP	Transmission Control Protocol
THx.y	THreat, where x and y represent numbers
TLS	Transport Layer Security
TPM	Trusted Platform Module
UC	Use Case
UEFI	Unified Extensible Firmware Interface
UI	User Interface
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
USB	Universal Serial Bus
VM	Virtual Machine
VPN	Virtual Private Network
XDR	eXtended Detection and Response
ZT	Zero Trust