



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

get full document from standards.iteh.ai

Reference

DEN/CYBER-EUS-0012

Keywords

CRA, cybersecurity, operating system

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	9
Foreword.....	9
Modal verbs terminology	10
Introduction	10
1 Scope	11
1.1 General.....	11
1.2 Products in scope	11
1.2.1 General	11
1.2.2 Components of operating systems that are in scope	12
1.3 Products covered by other CRA harmonised standards	12
2 References	13
2.1 Normative references	13
2.2 Informative references	14
3 Definition of terms, symbols and abbreviations	15
3.1 Terms	15
3.2 Symbols	17
3.3 Abbreviations.....	17
4 Product context.....	18
4.1 Intended purpose and reasonably foreseeable use	18
4.2 Product functions	18
4.3 Product architecture	19
4.3.1 Overview	19
4.3.2 Operating system security functions	19
4.3.3 Privileges.....	19
4.3.4 Access control mechanisms	19
4.3.5 Resource management.....	20
4.3.6 Scheduling.....	20
4.4 Operational Environment.....	20
4.5 Distribution of security functions	21
4.5.1 General	21
4.5.2 Security functions provided by some other part of its context	21
4.5.3 Security functions provided to other components	21
4.6 Users	21
4.7 Use cases.....	21
4.7.1 General	21
4.7.2 Basic use cases	22
4.7.2.1 UC-REST: Restricted operating system	22
4.7.2.2 UC-GEN: General-purpose operating system	22
4.7.3 Conditions	22
4.7.4 Characterising a product.....	23
4.7.5 Risk-factor levels of the basic use cases.....	23
4.8 Remote data-processing dependencies.....	24
4.8.1 General	24
4.8.2 Remote data-processing solutions	24
4.8.3 RDPS interfaces	24
4.8.4 RDPS-dependent product functions	25
5 Technical requirements for products	25
5.1 Notes on the structure of the Requirements	25
5.1.0 General	25
5.1.1 Necessity of Requirements	25
5.1.2 Types of Technical Requirements	25
5.1.3 Assumptions Regarding Requirements	26

5.1.3.1	Testability	26
5.1.3.2	Mitigations.....	26
5.1.3.3	Residual risk	26
5.2	Technical security requirements specifications	26
5.2.1	General	26
5.2.2	TR-NKEV: No known exploitable vulnerabilities	26
5.2.2.1	MI-KEVM: Documentation of mitigation of known exploitable vulnerabilities	26
5.2.2.2	MI-KEVT: Testing for known exploitable vulnerabilities	27
5.2.3	TR-MINI: Minimise impact on other devices and services.....	27
5.2.3.1	MI-RRIS: Document residual risk to other devices and services	27
5.2.3.2	MI-MNET: Minimise negative impact of network transmission.....	27
5.2.4	TR-SDEF: Secure by default configuration	27
5.2.4.1	MI-ADEF: Authorisation required by default to access security-relevant assets	27
5.2.4.2	MI-PDDI-1: Document how to control access to debug and management interfaces	28
5.2.4.3	MI-PDDI-2: Control local software access to debug and management interfaces	28
5.2.4.4	MI-PDDI-3: Control network access to debug or management interfaces	28
5.2.5	TR-SCUD: Secure updates.....	28
5.2.5.1	MI-KEVD: Documentation for secure update before or during first use	28
5.2.5.2	MI-KEVA: Secure update before or during first use	28
5.2.5.3	MI-SCUE: Security updates provided by the operational environment	29
5.2.5.4	MI-SUVI: Update authenticity and integrity verification.....	29
5.2.5.5	MI-SUDP: Anti-rollback protection	29
5.2.5.6	MI-SUAR: Authorised rollback	29
5.2.6	TR-AUTH: Authentication and access control	30
5.2.6.1	MI-RAUT: Authenticate the remote data processing solution and validate its interactions at the RDPS boundary	30
5.2.6.2	MI-AUTH-1: Require user authentication on interfaces providing access to the operating system	30
5.2.6.3	MI-AUTH-2: Require privilege or authorisation on interfaces providing access to the operating system	30
5.2.6.4	MI-LCKT: Authentication failure protection	30
5.2.6.5	MI-CRED: Protect stored critical security parameters and enforce credential strength	30
5.2.6.6	MI-ACCS: Access control enforcement on operating system resources and functions.....	31
5.2.6.7	MI-PRIV: Privilege separation and restriction	31
5.2.6.8	MI-SESS: Interactive session lifecycle controls.....	31
5.2.6.9	MI-ACSD: Access control for stored data.....	31
5.2.7	TR-CDST: Confidentiality of data stored on the product	31
5.2.7.1	MI-ENST: Cryptographic encryption of stored data	31
5.2.8	TR-CDTX: Confidentiality of data transmitted by the product.....	31
5.2.8.1	MI-CDTX: Protect confidentiality of user data transmitted by the product	31
5.2.8.2	MI-RRDC: Document residual risk to confidentiality of data transmitted	32
5.2.8.3	MI-ENTX: Cryptographic encryption of transmitted data	32
5.2.9	TR-CRYP: Encryption	32
5.2.9.1	MI-CRYP: Conformance to Annex K	32
5.2.10	TR-IDST: Integrity of data stored on the product	32
5.2.10.1	MI-DCST: Detect corruption of stored data	32
5.2.10.2	MI-INTS: Cryptographic integrity protection of stored data	32
5.2.11	TR-IDTX: Integrity of data transmitted by the product	33
5.2.11.1	MI-INTT: Cryptographic integrity protection of transmitted data	33
5.2.12	TR-DMIN: Data Minimisation.....	33
5.2.12.1	MI-DJST: Document and justify processed data	33
5.2.13	TR-AVAI: Availability	33
5.2.13.1	MI-AVNT: Availability of network functions.....	33
5.2.13.2	MI-CSFR: Detection and recovery from critical service failures	33
5.2.13.3	MI-RLIM: Resource usage limits and exhaustion fallback	34
5.2.13.4	MI-PRIO: Workload prioritisation	34
5.2.13.5	MI-RRDS: Document residual risk of denial of service.....	34
5.2.13.6	MI-RTDL: Real-time deadline preservation.....	34
5.2.13.7	MI-RTRY: Retry and degraded behaviour on unavailability of the remote data processing solution	34
5.2.14	TR-ISOL: Isolation	35
5.2.14.1	MI-ISO-1: Access control across security boundaries.....	35
5.2.14.2	MI-ISO-2: Process isolation	35

5.2.14.3	MI-ISO-3: Isolation between the processes of different users.....	35
5.2.14.4	MI-ISO-4: Isolation between the data of different users	35
5.2.14.5	MI-ISO-5: Privilege model.....	35
5.2.14.6	MI-ISO-6: Side-channel isolation.....	36
5.2.14.7	MI-ISO-7: Binary hardening	36
5.2.15	TR-LOGG: Logging and monitoring	36
5.2.15.1	MI-LOGG: Logging	36
5.2.16	TR-SCDL: Secure deletion	37
5.2.16.1	MI-SDEL: Secure deletion	37
5.2.16.2	MI-RRSD: Document residual risk to secure deletion	37
5.2.17	TR-SDTR: Secure data read and transfer.....	37
5.2.17.1	MI-SDRF: Secure data read from product.....	37
5.2.17.2	MI-SDTR: Document secure data transfer to another product or system.....	37
5.3	Security profiles.....	37
5.3.1	General.....	37
5.3.2	SP-REST baseline mitigations	38
5.3.3	SP-GEN baseline mitigations.....	38
5.3.4	Conditioned mitigations	39
5.3.4.0	General	39
5.3.4.1	C-NET: Public network access	39
5.3.4.2	C-NETR: Restricted network access	40
5.3.4.3	C-MOD: User-modifiable software, firmware, or hardware	40
5.3.4.4	C-APPS: Third-party application installation.....	40
5.3.4.5	C-LOSS: Loss or theft of a portable device.....	40
5.3.4.6	C-MULTI: Multiple user accounts	40
5.3.4.7	C-UNTR: Untrusted concurrent users	41
5.3.4.8	C-DATA: Sensitive or personal data	41
5.3.4.9	C-FUNC: Sensitive functions.....	41
5.3.4.10	C-RDPS: Remote data-processing dependency.....	42
5.3.4.11	C-PHYS: Physical exposure to untrusted persons.....	42
5.3.4.12	C-SELFADM: Self-administration.....	42
6	Assessment criteria for compliance with technical requirements	42
6.1	Introduction to the assessment and compliance criteria.....	42
6.2	TR-NKEV: No known exploitable vulnerabilities.....	44
6.2.1	[AC-KEVM] Assessment criteria: Documentation of mitigation of known exploitable vulnerabilities	44
6.2.2	[AC-KEVT] Assessment criteria: Testing for known exploitable vulnerabilities	45
6.3	TR-MINI: Minimise impact on other devices and services	45
6.3.1	[AC-RRIS] Assessment criteria: Document residual risk to other devices and services.....	45
6.3.2	[AC-MNET] Assessment criteria: Minimise negative impact of network transmission	46
6.4	TR-SDEF: Secure by default configuration.....	47
6.4.1	[AC-ADEF] Assessment criteria: Authorisation required by default to access security-relevant assets....	47
6.4.2	[AC-PDDI-1] Assessment criteria: Document how to control access to debug and management interfaces	48
6.4.3	[AC-PDDI-2] Assessment criteria: Control local software access to debug and management interfaces	48
6.4.4	[AC-PDDI-3] Assessment criteria: Control network access to debug or management interfaces.....	49
6.5	TR-SCUD: Secure updates	50
6.5.1	[AC-KEVD] Assessment criteria: Documentation for secure update before or during first use	50
6.5.2	[AC-KEVA] Assessment criteria: Secure update before or during first use	50
6.5.3	[AC-SCUE] Assessment criteria: Security updates provided by the operational environment	51
6.5.4	[AC-SUVI] Assessment criteria: Update authenticity and integrity verification	52
6.5.5	[AC-SUDP] Assessment criteria: Anti-rollback protection	53
6.5.6	[AC-SUAR] Assessment criteria: Authorised rollback.....	53
6.6	TR-AUTH: Authentication and access control	54
6.6.1	[AC-RAUT] Assessment criteria: Authenticate the remote data processing solution and validate its interactions at the RDPS boundary	54
6.6.2	[AC-AUTH-1] Assessment criteria: Require user authentication on interfaces providing access to the operating system.....	55
6.6.3	[AC-AUTH-2] Assessment criteria: Require privilege or authorisation on interfaces providing access to the operating system.....	56
6.6.4	[AC-LCKT] Assessment criteria: Authentication failure protection.....	57

6.6.5	[AC-CRED] Assessment criteria: Protect stored critical security parameters and enforce credential strength.....	57
6.6.6	[AC-ACCS] Assessment criteria: Access control enforcement on operating system resources and functions.....	58
6.6.7	[AC-PRIV] Assessment criteria: Privilege separation and restriction.....	59
6.6.8	[AC-SESS] Assessment criteria: Interactive session lifecycle controls	60
6.6.9	[AC-ACSD] Assessment criteria: Access control for stored data	61
6.7	TR-CDST: Confidentiality of data stored on the product.....	62
6.7.1	[AC-ENST] Assessment criteria: Cryptographic encryption of stored data.....	62
6.8	TR-CDTX: Confidentiality of data transmitted by the product	63
6.8.1	[AC-CDTX] Assessment criteria: Protect confidentiality of user data transmitted by the product.....	63
6.8.2	[AC-RRDC] Assessment criteria: Document residual risk to confidentiality of data transmitted	64
6.8.3	[AC-ENTX] Assessment criteria: Cryptographic encryption of transmitted data	64
6.9	TR-CRYP: Encryption.....	65
6.9.1	[AC-CRYP] Assessment criteria: Conformance to Annex K.....	65
6.10	TR-IDST: Integrity of data stored on the product.....	66
6.10.1	[AC-DCST] Assessment criteria: Detect corruption of stored data	66
6.10.2	[AC-INTS] Assessment criteria: Cryptographic integrity protection of stored data	66
6.11	TR-IDTX: Integrity of data transmitted by the product.....	67
6.11.1	[AC-INTT] Assessment criteria: Cryptographic integrity protection of transmitted data	67
6.12	TR-DMIN: Data Minimisation	68
6.12.1	[AC-DJST] Assessment criteria: Document and justify processed data	68
6.13	TR-AVAI: Availability.....	69
6.13.1	[AC-AVNT] Assessment criteria: Availability of network functions.....	69
6.13.2	[AC-CSFR] Assessment criteria: Detection and recovery from critical service failures	70
6.13.3	[AC-RLIM] Assessment criteria: Resource usage limits and exhaustion fallback.....	70
6.13.4	[AC-PRIO] Assessment criteria: Workload prioritisation.....	71
6.13.5	[AC-RRDS] Assessment criteria: Document residual risk of denial of service	72
6.13.6	[AC-RTDL] Assessment criteria: Real-time deadline preservation	73
6.13.7	[AC-RTRY] Assessment criteria: Retry and degraded behaviour on unavailability of the remote data processing solution.....	73
6.14	TR-ISOL: Isolation	74
6.14.1	[AC-ISO-1] Assessment criteria: Access control across security boundaries	74
6.14.2	[AC-ISO-2] Assessment criteria: Process isolation.....	75
6.14.3	[AC-ISO-3] Assessment criteria: Isolation between the processes of different users	76
6.14.4	[AC-ISO-4] Assessment criteria: Isolation between the data of different users.....	77
6.14.5	[AC-ISO-5] Assessment criteria: Privilege model	77
6.14.6	[AC-ISO-6] Assessment criteria: Side-channel isolation.....	78
6.14.7	[AC-ISO-7] Assessment criteria: Binary hardening.....	80
6.15	TR-LOGG: Logging and monitoring.....	81
6.15.1	[AC-LOGG] Assessment criteria: Logging.....	81
6.16	TR-SCDL: Secure deletion	82
6.16.1	[AC-SDEL] Assessment criteria: Secure deletion.....	82
6.16.2	[AC-RRSD] Assessment criteria: Document residual risk to secure deletion.....	83
6.17	TR-SDTR: Secure data read and transfer	83
6.17.1	[AC-SDRF] Assessment criteria: Secure data read from product	83
6.17.2	[AC-SDTR] Assessment criteria: Document secure data transfer to another product or system	84

Annex A (informative):	Relationship between the present document and the essential cybersecurity requirements of Regulation (EU) 2024/2847	86
-------------------------------	--	-----------

Annex B (informative):	Security analysis.....	88
-------------------------------	-------------------------------	-----------

B.0	General	88
B.1	Assets	88
B.1.1	Data assets	88
B.1.2	Software assets.....	88
B.1.3	Hardware-interfacing assets.....	88
B.1.4	Network assets	89
B.1.5	Identity and access assets.....	89
B.1.6	Product functions.....	89
B.1.7	Impact of asset compromise.....	89

B.2	Risk factors.....	90
B.2.1	General comments regarding risk factors	90
B.2.2	RF-NUSR: Number of User Accounts	90
B.2.3	RF-CUSR: User Account Concurrency	90
B.2.4	RF-PPII: Potential for Collection of Personally Identifiable Information	91
B.2.5	RF-SNDS: Sensitivity of Data Stored.....	91
B.2.6	RF-SNDT: Sensitivity of Data Transmitted.....	91
B.2.7	RF-SENF: Sensitivity of Functions	91
B.2.8	RF-PHYS: Physical Access by Threat Actors to the Device	91
B.2.9	RF-UEIN: Processing of Untrusted External Inputs	91
B.2.10	RF-LOSS: Probability of Loss of the Device	92
B.2.11	RF-HWMD: Hardware Modifiability by End Users.....	92
B.2.12	RF-SWMD: Software Modifiability by End Users.....	92
B.2.13	RF-DVCS: Untrusted Peripheral Devices.....	92
B.2.14	RF-TNET: Access to a Public Network.....	92
B.2.15	RF-FNET: Accessed From Untrusted Networks Including a Public Network	93
B.2.16	RF-CONF: Configurability	93
B.2.17	RF-ADMN: Administration.....	93
B.2.18	RF-SUPP: Support and Foreseeable Updates	93
B.2.19	RF-RDPS: Remote data processing dependency	93
B.3	Assumptions.....	94
B.3.0	General.....	94
B.3.1	AS-PA: Proper administrator	94
B.4	Security analysis.....	94
B.4.1	Methodology.....	94
B.4.2	TH-UEVU: Unknown exploitable vulnerabilities	94
B.4.3	TH-KEVU: Known exploitable vulnerabilities	95
B.4.4	TH-SUPC: Compromise of the secure update mechanism	95
B.4.5	TH-UAPP: Unauthorised access to product assets via unprotected physical interfaces in default configuration.....	96
B.4.6	TH-UAPS: Unauthorised access to product assets via unprotected local software access in default configuration.....	97
B.4.7	TH-UAPN: Unauthorised access to product assets via unprotected network interfaces in default configuration.....	97
B.4.8	TH-UADT: Unauthorised access to confidential data transmitted	98
B.4.9	TH-UADX: Unauthorised access to data during transfer to another product	98
B.4.10	TH-PDOS: Denial of service attack on product functions via user or network access	99
B.4.11	TH-DDOS: Denial of service attack on other products via exploitation of vulnerabilities or unauthorised use of product functions.....	100
B.4.12	TH-MQSE: Masquerading authorised server	100
B.4.13	TH-XUSR: Unauthorised access, resource exhaustion, or privilege escalation between concurrent users ...	101
B.4.14	TH-LEAK: Data leak through side channels	101
B.4.15	TH-RDPS: Compromise of the remote data processing solution boundary.....	102
B.4.16	TH-SUPP: Supply chain compromise.....	102
B.4.17	TH-HARD: Compromise via hardware-level or platform trust components.....	103
B.5	Mapping of use cases to risk factors	103
B.5.1	General.....	103
B.5.2	Baseline risk-factor levels of the basic use cases.....	103
B.5.3	Condition increments.....	104
B.5.4	Deriving the risk profile of a product.....	104
B.6	Security profiles	104
B.6.1	General.....	104
B.6.2	Mapping of security profiles to risk factors	105
B.6.3	Determining the applicable mitigations	105
B.6.4	Relationship to the threat analysis	106
Annexes C to J: Void.....		107

Annex K (normative):	Generic requirements and assessment criteria for the use of state of the art cryptography.....	108
K.0	General	108
K.1	Cryptography.....	108
K.1.1	Requirement.....	108
K.1.2	Assessment of product cryptographic configuration.....	109
K.1.2.0	General	109
K.1.2.1	Assessment of ACM-listed cryptographic mechanisms	109
K.1.2.1.1	Assessment objective.....	109
K.1.2.1.2	Assessment preparation	109
K.1.2.1.3	Assessment activities	110
K.1.2.1.4	Assessment evidence	110
K.1.2.1.5	Assessment verdict	110
K.1.2.2	Assessment of ACM-extended cryptographic mechanisms	110
K.1.2.2.1	Assessment objective.....	110
K.1.2.2.2	Assessment preparation	110
K.1.2.2.3	Assessment activities	110
K.1.2.2.4	Assessment evidence	111
K.1.2.2.5	Assessment verdict	111
K.1.2.3	Assessment of interoperability-based cryptographic mechanisms	111
K.1.2.3.1	Assessment objective.....	111
K.1.2.3.2	Assessment preparation	111
K.1.2.3.3	Assessment activities	112
K.1.2.3.4	Assessment evidence	112
K.1.2.3.5	Assessment verdict	112
K.2	Crypto agility	113
K.2.1	Requirement.....	113
K.2.2	Assessment of crypto-agility.....	113
K.2.2.1	Assessment objective	113
K.2.2.2	Assessment preparation.....	114
K.2.2.3	Assessment activities.....	114
K.2.2.4	Assessment evidence.....	114
K.2.2.5	Assessment verdict.....	114
K.3	ACM-extended cryptographic mechanisms	115
K.3.1	Requirement.....	115
K.3.2	List of ACM-extended cryptographic mechanisms	115
K.3.3	Assessment	117
K.4	Interoperability-based cryptographic mechanisms.....	117
K.4.1	Requirement.....	117
K.4.2	List of interoperability-based cryptographic mechanisms	117
K.4.3	Assessment	119
Annex L (informative):	Change history	120
History		121

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.

BLUETOOTH® is a trademark registered and owned by Bluetooth SIG, Inc.

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 defines cybersecurity requirements for operating systems. These products are identified in Annex III, Class I, point 11 of Regulation (EU) 2024/2847 [i.1], the Cyber Resilience Act, referred to as "CRA".

The present document supports compliance with the CRA [i.1] by addressing the essential cybersecurity requirements defined in Annex I, Part I of the CRA [i.1], and provides a structured approach to identify the applicable cybersecurity requirements for the operating systems in scope, following a risk-based approach. The security measures and controls are thereby proportionate to the intended purpose, reasonably foreseeable use, deployment context, and threat exposure of the product. The present document is intended for manufacturers of operating systems and for the bodies that assess their conformity.

Clause 4 describes the product architecture and intended purpose in their context, and defines the use cases used to characterise the operating systems in scope. A product corresponds to exactly one basic use case, namely a restricted operating system (UC-REST) or a general-purpose computing platform (UC-GEN), together with any conditions that hold for it. The basic use case and the conditions reflect the reasonably foreseeable use of the product and serve as the basis for identifying the relevant cybersecurity risks. Clause 4.8 identifies dependencies on remote data-processing solutions.

Clause 5 specifies the technical cybersecurity requirements for the product. Each requirement is grouped under a technical requirement (TR-XXX) and is expressed as one or more mitigations (MI-XXX). Clause 5.3 defines the two security profiles, SP-REST and SP-GEN, one for each basic use case; a product is assigned the security profile of its basic use case. The mitigations that apply to a given product are the baseline mitigations of its security profile together with the mitigations carried by each condition that holds for the product.

Clause 6 defines the conformity assessment activities for each mitigation in clause 5.

Annex A maps the technical requirements of the present document to the essential cybersecurity requirements of the CRA.

Annex B describes the risk identification and assessment methodology used to derive the security profiles in clause 5.3 and the conditions in clause 4.7. It records the baseline risk-factor levels of the basic use cases and the risk-factor increments contributed by each condition, from which the applicable mitigations are determined.

Annex K specifies the requirement for the use of state of the art cryptography, the assessment of the product's cryptographic configuration, and the crypto-agility requirement. It classifies cryptographic mechanisms as state of the art and lists the cryptographic mechanisms recognised by the present document in addition to the ACM catalogue.

1 Scope

1.1 General

The present document specifies technical requirements and corresponding assessment criteria for operating systems related to cybersecurity. The products with digital elements in scope, thereafter "the operating system":

- are specified within the "technical description" of the "category of product" number 11 of Annex III, Class I by the Commission Implementing Regulation (EU) 2025/2392 [i.2] as:
"software products with digital elements that provide an abstract interface of the underlying hardware and control the execution of software, and that may provide services such as computing resource management and configuration, scheduling, input-output control, managing data, and providing an interface through which applications interact with system resources and peripherals. This category includes but is not limited to real-time operating systems, general-purpose and special-purpose operating systems".
- 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 use of harmonised standards is voluntary.

1.2 Products in scope

1.2.1 General

Products in scope are products whose core function and intended or reasonably foreseeable use or misuse is as an operating system. Operating systems are defined in point 11 of Annex III, Class I of Regulation (EU) 2024/2847 [i.1] and described in Commission Implementing Regulation (EU) 2025/2392 [i.2] as "software products with digital elements that provide an abstract interface of the underlying hardware and control the execution of software, and that may provide services such as computing resource management and configuration, scheduling, input-output control, managing data, and providing an interface through which applications interact with system resources and peripherals. This category includes but is not limited to real-time operating systems, general-purpose and special-purpose operating systems".

The present document applies equally to real-time, general-purpose, and special-purpose operating systems. Where a specific requirement depends on hardware or software features that not all operating system architectures provide, the applicability of that requirement is stated in the applicability field of the corresponding mitigation in clause 5.

The underlying hardware may be virtualised to some degree, as when an operating system is running on a hypervisor.

This category includes but is not limited to:

- General purpose operating systems
 - Personal computing operating systems
 - Mobile operating systems
 - Server operating systems
- Special purpose operating systems
 - Real-time operating systems
 - Embedded operating systems
 - Single-purpose operating systems

Many products contain multiple operating systems which can affect the security functions of other operating system(s) in the product. For example, a Baseboard Management Controller (BMC) contains an operating system that can manage most or all of the hardware managed by the main system operating system. Radiofrequency transmission devices often have an embedded real-time operating system and the ability to read or write to system memory or trigger interrupts.

Where a product contains multiple operating systems, the present document applies to each operating system in scope separately. From the perspective of the operating system under assessment, any other operating system in the product is part of its operational environment.

Some of the operating systems may not always be readily available as separate products and are included as components of another product. Where there may be other specifications that target that product category, it may be more relevant to review the operating system as part of that larger system rather than independently via the present document.

1.2.2 Components of operating systems that are in scope

The present document applies to the operating system as a whole. The following non-exhaustive list identifies common component types where the cybersecurity requirements of the present document most often have effect. The list is informative; all components of the operating system are covered by the requirements.

The following non-exhaustive list of types of components are common to many operating systems and, when present, are considered security-relevant:

- **Kernel:** The central component responsible for managing hardware resources and enforcing access controls.
- **Device Drivers:** Software components supplied with the operating system that interact directly with hardware devices.
- **Cybersecurity Libraries:** Libraries used to provide cybersecurity services, such as encryption, authentication, and authorisation.
- **Authentication Services:** Authentication mechanisms required for operating system functionality.
- **Privileged Processes:** Operating system processes running with elevated privileges or access to sensitive resources.
- **Software Update Mechanisms:** Systems responsible for installing and updating software components supplied with the operating system.
- **Logging and Monitoring:** Functions performed by the operating system that record cybersecurity-relevant events or monitor system behaviour.
- **Configuration Management:** Management of the configuration of cybersecurity-relevant operating system settings, including provisioning of a secure-by-default configuration.

A given component may fall under more than one category. The categories are illustrative and not mutually exclusive.

1.3 Products covered by other CRA harmonised standards

Some product categories that provide functionality overlapping with an operating system are covered by their own CRA harmonised standard. Where such a standard exists for a product category, that standard applies to it. These categories include:

- Hypervisors and container runtime systems that support virtualised execution of operating systems (Annex III, Class II, point 1 of Regulation (EU) 2024/2847 [i.1]).
- Boot managers (Annex III, Class I, point 8 of Regulation (EU) 2024/2847 [i.1]).

For products that embed or interact with an operating system while having a different core functionality, manufacturers may refer to the present document as one part of demonstrating compliance for the operating system component.

2 References

2.1 Normative references

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

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

The following referenced documents 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] [BSI TR-02102-1](#) (Version 2026-01, 23 January 2026): "Cryptographic Mechanisms: Recommendations and Key Lengths".
- [3] [NIST SP 800-108 Rev. 1 \(August 2022\)](#): "Recommendation for Key Derivation Using Pseudorandom Functions".
- [4] [NIST SP 800-131A Rev. 2 \(March 2019\)](#): "Transitioning the Use of Cryptographic Algorithms and Key Lengths".
- [5] [Canadian Centre for Cyber Security ITSP.40.062](#): "Guidance on Securely Configuring Network Protocols".
- [6] [IRTF RFC 7748 \(January 2016\)](#): "Elliptic Curves for Security".
- [7] [IRTF RFC 8032 \(January 2017\)](#): "Edwards-Curve Digital Signature Algorithm (EdDSA)".
- [8] [IETF RFC 8410 \(August 2018\)](#): "Algorithm Identifiers for Ed25519, Ed448, X25519, and X448 for Use in the Internet X.509 Public Key Infrastructure".
- [9] [IRTF RFC 8439 \(June 2018\)](#): "ChaCha20 and Poly1305 for IETF Protocols".
- [10] [IRTF RFC 9106 \(September 2021\)](#): "Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications".
- [11] [IETF RFC 7914 \(August 2016\)](#): "The scrypt Password-Based Key Derivation Function".
- [12] [IETF RFC 1321 \(April 1992\)](#): "The MD5 Message-Digest Algorithm".
- [13] [IETF RFC 3174 \(September 2001\)](#): "US Secure Hash Algorithm 1 (SHA1)".
- [14] [NIST SP 800-132 \(December 2010\)](#): "Recommendation for Password-Based Key Derivation, Part 1: Storage Applications".
- [15] [IETF RFC 2268 \(March 1998\)](#): "A Description of the RC2(r) Encryption Algorithm".
- [16] [IETF RFC 7465 \(February 2015\)](#): "Prohibiting RC4 Cipher Suites".
- [17] [IETF RFC 6229 \(May 2011\)](#): "Test Vectors for the Stream Cipher RC4".
- [18] [FIPS PUB 186-5 \(February 2023\)](#): "Digital Signature Standard (DSS)".
- [19] SEC2 SEC 2: "[Recommended Elliptic Curve Domain Parameters](#)", [Version 2.0, January 2010](#).
- [20] [NIST SP 800-135 Rev. 1 \(December 2011\)](#): "Recommendation for Existing Application-Specific Key Derivation Functions".
- [21] [FIPS PUB 180-4 \(August 2015\)](#): "Secure Hash Standard (SHS)".
- [22] [FIPS PUB 198-1 \(July 2008\)](#): "The Keyed-Hash Message Authentication Code (HMAC)".

2.2 Informative references

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

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

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

- [i.1] [Regulation \(EU\) 2024/2847](#) of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).
 - [i.2] [Commission Implementing Regulation \(EU\) 2025/2392](#) of 28 November 2025 on the technical description of the categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of the Council.
 - [i.3] [Standardisation request M/606 - C\(2025\)618](#): "Commission Implementing decision of 3.2.2025 on a standardisation request to the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)".
 - [i.4] prEN 40000-1-1: "Cybersecurity requirements for products with digital elements - Vocabulary", (produced by CEN/CENELEC).
- NOTE: Version and date to be added upon its publication by CEN/CENELEC.
- [i.5] ETSI EN 303 645: "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".
 - [i.6] EN 18031 series: "Common security requirements for radio equipment" (produced by CEN/CENELEC).
 - [i.7] CEN/CLC JTC13: "Cybersecurity and Data Protection".
 - [i.8] ISO/IEC 15408: "Information security, cybersecurity and privacy protection - Evaluation criteria for IT security".
 - [i.9] BSI CC-PP-0067: "Operating System Protection Profile".
 - [i.10] ISO 31000: "Risk management - Guidelines".
 - [i.11] IETF RFC 4987: "TCP SYN Flooding Attacks and Common Mitigations".
 - [i.12] ANSSI: "Recommendations for the secure configuration of a GNU/Linux system", Version 2.0.
 - [i.13] FIPS PUB 46-3 (October 1999): "Data Encryption Standard (DES)".
 - [i.14] 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.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in prEN 40000-1-1 [i.4] and the following apply:

NOTE: This clause provides terms and definitions based on CEN/CLC JTC13 WG09's [i.7] work on terms and definitions, terms and definitions provided by ETSI EN 303 645 [i.5] and by EN 18031 [i.6] series, and informed by terms used in the Common Criteria [i.8] and the NIAP Operating System Protection Plan [i.9] guide.

administrator: entity that is responsible for management activities, including setting policies that are applied by the enterprise on the operating system

NOTE: This administrator could be acting remotely through a management server, from which the system receives configuration policies. An administrator can enforce settings on the system which cannot be overridden by non-administrator users.

application: software that runs on a platform and performs tasks on behalf of the user or owner of the platform, as well as its supporting documentation

Application Programming Interface (API): specification of routines, data structures, object classes, and variables that allows an application to make use of services provided by another software component, such as a library

NOTE: APIs are often provided for a set of libraries included with the platform.

attack surface: user interfaces, target protocol interfaces and reachable data paths that can be attacked from inside or outside the system

command shell: text-based interface allowing execution of system programs

Common Criteria (CC): criteria for the evaluation of information technology security specified in ISO/IEC 15408 [i.8]

Common Weakness Enumeration (CWE): community-developed list of software and hardware weaknesses that can become vulnerabilities

compensating control: alternative control that meets the intent and rigour of a prescribed control when the prescribed control cannot be implemented for legitimate technical or business reasons

core function: function that is fundamental to the operation of the operating system, such as process scheduling, memory management, and input-output control, and whose loss of availability constitutes a denial-of-service condition

credential: data that establishes the identity of a user, e.g. a cryptographic key or password

cryptographic mechanism: security-related procedure using cryptography

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

NOTE 2: 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 and 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: Cryptographic properties include, for example, confidentiality, integrity, authenticity, entity authentication, message authentication, key establishment, key confirmation, replay protection, collision resistance, preimage resistance, signature unforgeability, non-repudiation, and forward secrecy. Where relevant, a cryptographic property can be expressed using a formal cryptographic notion, for example IND-CPA, IND-CCA2, EUF-CMA or SUF-CMA.