



**Cyber Security (CYBER); CRA;
Cybersecurity requirements for physical and
virtual network interfaces**

get full document from standards.iteh.ai

ReferenceDEN/CYBER-EUS-0017

KeywordsCRA, cybersecurity, interface

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	15
Foreword.....	15
Modal verbs terminology.....	16
Introduction	16
1 Scope	17
2 References	17
2.1 Normative references	17
2.2 Informative references.....	18
3 Definition of terms, symbols and abbreviations.....	19
3.1 Terms.....	19
3.2 Symbols.....	20
3.3 Abbreviations	20
4 Product context.....	20
4.0 Introduction	20
4.1 Product Functions.....	21
4.1.1 Physical network interface product functions	21
4.1.2 Device driver product functions.....	22
4.1.3 Virtual network interface product functions	22
4.2 Product Architecture.....	22
4.2.1 Overview	22
4.2.2 Types of network interface	22
4.2.3 Device drivers for network interfaces	24
4.3 Operational Environment	25
4.3.1 General description	25
4.3.2 Physical/Hardware environment	25
4.3.3 Logical/Software environment.....	25
4.3.4 Connectivity aspects	26
4.4 Distribution of Security Functions	26
4.4.1 General.....	26
4.4.2 Security functions provided outside the product.....	26
4.4.3 Security functions provided to other components.....	26
4.5 Users.....	27
4.6 Use Cases	27
4.6.1 Introduction.....	27
4.6.1.1 Overview	27
4.6.1.2 Guidance	28
4.6.2 Use case descriptions	28
4.6.2.1 UC-VI-ISO: Virtual interface for research within a host system	28
4.6.2.2 UC-PH-VNI: Vending machine internal network.....	28
4.6.2.3 UC-PH-VNC: Vending machine, remotely managed	29
4.6.2.4 UC-PH-IOT: Physical network interface for home IoT	29
4.6.2.5 UC-PH-IRO: Intranet router.....	29
4.6.2.6 UC-PH-EDG: Edge router	30
4.6.2.7 UC-PH-HRO: Home router in filtered network	30
4.6.2.8 UC-PH-ISP: ISP access point	30
4.6.2.9 UC-VI-VDC: Virtualize data centre	31
4.6.2.10 UC-VI-VMW: VM on multi-tenant web server	31
4.6.2.11 UC-VI-VMC: Virtualize critical server	31
4.6.2.12 UC-VI-VII: Virtual interface for integrators.....	32
4.6.2.13 UC-PH-SMW: Smart watch.....	32
4.6.2.14 UC-PH-SME: Smart meter	33
4.6.2.15 UC-PH-ATM: ATM.....	33
4.6.2.16 UC-PH-SPI: Solar panel inverter	33
4.6.2.17 UC-VI-VPN: Consumer VPN.....	34

4.6.2.18	UC-PH-MOB: Mobile phone or tablet.....	34
4.6.2.19	UC-PH-GPI: General purpose integrated.....	34
4.6.2.20	UC-PH-USB: External USB	35
4.6.2.21	UC-PH-STA: Standalone.....	35
4.6.2.22	UC-PH-SNS: Remote Sensor.....	35
5	Technical requirements for products.....	36
5.1	Introduction	36
5.1.1	Applicability of the requirements	36
5.1.2	Applicability of Annex K	36
5.1.3	Applicability of Annex R.....	36
5.1.4	Guidance for "cybersecurity-relevant".....	36
5.2	Appropriate level of cybersecurity	37
5.2.1	Overview	37
5.2.1.1	CRA Relevance.....	37
5.2.2	REQ-ALC-01 Resilience to potentially untrusted inputs.....	37
5.2.2.1	Requirement	37
5.2.2.2	Applicability.....	37
5.2.3	Mapping of requirements to use cases	38
5.3	No known exploitable vulnerabilities.....	38
5.3.1	Overview	38
5.3.2	REQ-KEV-01 No known exploitable vulnerabilities	38
5.3.2.1	Requirement	38
5.3.2.2	Applicability.....	38
5.3.2.3	Guidance	39
5.3.3	Mapping of requirements to use cases	40
5.4	Secure by default configuration.....	40
5.4.1	Overview	40
5.4.2	REQ-SBD-01: Provide methods to protect or disable interfaces.....	40
5.4.2.1	Requirement	40
5.4.2.2	Applicability.....	40
5.4.2.3	Guidance	41
5.4.3	REQ-SBD-02: Protect or disable access to debug or management interfaces	41
5.4.3.1	Requirement	41
5.4.3.2	Applicability.....	41
5.4.3.3	Guidance	42
5.4.4	Mapping of requirements to use cases	42
5.5	Security updates	42
5.5.1	Overview	42
5.5.2	REQ-SU-01: Secure update provided by operational environment	43
5.5.2.1	Requirement	43
5.5.2.2	Applicability.....	43
5.5.3	Mapping of requirements to use cases	44
5.6	Authentication and access control.....	44
5.6.1	Overview	44
5.6.2	REQ-AAC-01: Authentication and access control provided by operational environment.....	44
5.6.2.1	Requirement	44
5.6.2.2	Applicability.....	44
5.6.3	Mapping of requirements to use cases	45
5.7	Confidentiality protection.....	46
5.7.1	Overview	46
5.7.2	REQ-CP-01: Confidentiality protection provided by operational environment.....	46
5.7.2.1	Requirement	46
5.7.2.2	Applicability.....	46
5.7.2.3	Guidance	47
5.7.3	Mapping of requirements to use cases	47
5.8	Integrity protection	47
5.8.1	Overview	47
5.8.2	REQ-IP-01: Integrity protection provided by operational environment	47
5.8.2.1	Requirement	47
5.8.2.2	Applicability.....	47
5.8.3	Mapping of requirements to use cases	48

5.9	Data minimisation	49
5.9.1	Overview	49
5.9.2	REQ-DM-01: Data minimisation.....	49
5.9.2.1	Requirement	49
5.9.2.2	Applicability.....	49
5.9.3	Mapping of requirements to use cases	50
5.10	Availability protection.....	50
5.10.1	Overview	50
5.10.2	REQ-AP-01 Fast packet drop	50
5.10.2.1	Requirement	50
5.10.2.2	Applicability.....	50
5.10.2.3	Guidance	51
5.10.3	REQ-AP-02 Limit resource usage by incoming network data.....	51
5.10.3.1	Requirement	51
5.10.3.2	Applicability.....	51
5.10.4	REQ-AP-03 Availability protection provided by operational environment.....	52
5.10.4.1	Requirement	52
5.10.4.2	Applicability.....	52
5.10.5	REQ-AP-04: Watchdog and notification of host	53
5.10.5.1	Requirement	53
5.10.5.2	Applicability.....	53
5.10.6	REQ-AP-05: Watchdog and self-initiated reset.....	54
5.10.6.1	Requirement	54
5.10.6.2	Applicability.....	54
5.10.7	Mapping of requirements to use cases	55
5.11	Non-interference.....	55
5.11.1	Overview	55
5.11.2	REQ-NI-01: Minimise data transmitted to unverified sources	55
5.11.2.1	Requirement	55
5.11.2.2	Applicability.....	55
5.11.2.3	Guidance	56
5.11.3	Mapping of requirements to use cases	57
5.12	Attack surface minimisation.....	57
5.12.1	Overview	57
5.12.2	REQ-ASM-01: Minimise attack surface.....	57
5.12.2.1	Requirement	57
5.12.2.2	Applicability.....	57
5.12.3	Mapping of requirements to use cases	58
5.13	Exploit mitigation.....	58
5.13.1	Overview	58
5.13.2	Requirements	58
5.13.3	Mapping of requirements to use cases	59
5.14	Monitoring.....	59
5.14.1	Overview	59
5.14.2	REQ-MON-01: Logging.....	59
5.14.2.1	Requirement	59
5.14.2.2	Applicability.....	59
5.14.3	Mapping of requirements to use cases	60
5.15	Factory reset and data portability	60
5.15.1	Overview	60
5.15.2	REQ-SDT-01 Secure deletion.....	61
5.15.2.1	Requirement	61
5.15.2.2	Applicability.....	61
5.15.3	REQ-SDT-02 Secure data read provided by operational environment.....	62
5.15.3.1	Requirement	62
5.15.3.2	Applicability.....	62
5.15.4	Mapping of requirements to use cases	63
6	Assessment criteria for compliance with technical requirements	63
6.1	Introduction to the assessment and compliance criteria	63
6.1.1	General.....	63
6.1.2	Guidance for identifying interfaces or data processing.....	65

6.2	Appropriate level of cybersecurity	65
6.2.1	Overview	65
6.2.2	REQ-ALC-01 Resilience to potentially untrusted inputs.....	65
6.2.2.1	Objective	65
6.2.2.2	Preparation	66
6.2.2.3	Activities	67
6.2.2.4	Verdict.....	67
6.2.2.5	Evidence.....	67
6.2.2.6	Guidance	67
6.3	No known exploitable vulnerabilities.....	68
6.3.1	Overview	68
6.3.2	REQ-KEV-01 No known exploitable vulnerabilities	68
6.3.2.1	Objective	68
6.3.2.2	Preparation	68
6.3.2.3	Activities	68
6.3.2.4	Verdict.....	68
6.3.2.5	Evidence.....	68
6.3.2.6	Guidance	69
6.4	Secure by default configuration.....	69
6.4.1	Overview	69
6.4.2	REQ-SBD-01: Provide methods to protect or disable interfaces.....	69
6.4.2.1	Objective	69
6.4.2.2	Preparation	69
6.4.2.3	Activities	69
6.4.2.4	Verdict.....	69
6.4.2.5	Evidence.....	70
6.4.2.6	Guidance	70
6.4.3	REQ-SBD-02: Protect or disable access to debug or management interfaces	70
6.4.3.1	Objective	70
6.4.3.2	Preparation	70
6.4.3.3	Activities	70
6.4.3.4	Verdict.....	70
6.4.3.5	Evidence.....	71
6.5	Security updates	71
6.5.1	Overview	71
6.5.2	REQ-SU-01 Secure update provided by operational environment	71
6.5.2.1	Objective	71
6.5.2.2	Preparation	71
6.5.2.3	Activities	71
6.5.2.4	Verdict.....	71
6.5.2.5	Evidence.....	71
6.5.2.6	Guidance	72
6.6	Authentication and access control	72
6.6.1	Overview	72
6.6.2	REQ-AAC-01: Authentication and access control provided by operational environment.....	72
6.6.2.1	Objective	72
6.6.2.2	Preparation	72
6.6.2.3	Activities	72
6.6.2.4	Verdict.....	72
6.6.2.5	Evidence.....	72
6.7	Confidentiality protection.....	72
6.7.1	Overview	72
6.7.2	REQ-CP-01: Confidentiality protection provided by operational environment.....	73
6.7.2.1	Objective	73
6.7.2.2	Preparation	73
6.7.2.3	Activities	73
6.7.2.4	Verdict.....	73
6.7.2.5	Evidence.....	73
6.7.2.6	Guidance	73
6.8	Integrity protection.....	74
6.8.1	Overview	74
6.8.2	REQ-IP-01: Integrity protection provided by operational environment	74

6.8.2.1	Objective	74
6.8.2.2	Preparation	74
6.8.2.3	Activities	74
6.8.2.4	Verdict.....	74
6.8.2.5	Evidence.....	74
6.8.2.6	Guidance	74
6.9	Data minimisation	75
6.9.1	Overview	75
6.9.2	REQ-DM-01: Minimise data processed.....	75
6.9.2.1	Objective	75
6.9.2.2	Preparation	75
6.9.2.3	Activities	75
6.9.2.4	Verdict.....	75
6.9.2.5	Evidence.....	75
6.9.2.6	Guidance	76
6.10	Availability protection.....	76
6.10.1	Overview	76
6.10.2	REQ-AP-01 Fast packet drop	76
6.10.2.1	Objective	76
6.10.2.2	Preparation	76
6.10.2.3	Activities	76
6.10.2.4	Verdict.....	76
6.10.2.5	Evidence.....	77
6.10.2.6	Guidance	77
6.10.3	REQ-AP-02 Limit resource usage by incoming network data.....	77
6.10.3.1	Objective	77
6.10.3.2	Preparation	77
6.10.3.3	Activities	77
6.10.3.4	Verdict.....	77
6.10.3.5	Evidence.....	77
6.10.3.6	Guidance	78
6.10.4	REQ-AP-03 Availability protection provided by operational environment.....	78
6.10.4.1	Objective	78
6.10.4.2	Preparation	78
6.10.4.3	Activities	78
6.10.4.4	Verdict.....	78
6.10.4.5	Evidence.....	79
6.10.4.6	Guidance	79
6.10.5	REQ-AP-04: Watchdog and notification of host	79
6.10.5.1	Objective	79
6.10.5.2	Preparation	79
6.10.5.3	Activities	79
6.10.5.4	Verdict.....	79
6.10.5.5	Evidence.....	79
6.10.5.6	Guidance	79
6.10.6	REQ-AP-05: Watchdog and self-initiated reset.....	79
6.10.6.1	Objective	79
6.10.6.2	Preparation	80
6.10.6.3	Activities	80
6.10.6.4	Verdict.....	80
6.10.6.5	Evidence.....	80
6.11	Non-interference.....	80
6.11.1	Overview	80
6.11.2	REQ-NI-01: Minimise data transmitted to unverified sources	80
6.11.2.1	Objective	80
6.11.2.2	Preparation	80
6.11.2.3	Activities	80
6.11.2.4	Verdict.....	80
6.11.2.5	Evidence.....	81
6.12	Attack surface minimisation.....	81
6.12.1	Overview	81
6.12.2	REQ-ASM-01: Minimise attack surface.....	81

6.12.2.1	Objective	81
6.12.2.2	Preparation	81
6.12.2.3	Activities	81
6.12.2.4	Verdict.....	81
6.12.2.5	Evidence.....	81
6.12.2.6	Guidance	82
6.13	Exploit mitigation.....	82
6.13.1	Overview	82
6.14	Monitoring.....	82
6.14.1	Overview	82
6.14.2	REQ-MON-01 Logging.....	82
6.14.2.1	Objective	82
6.14.2.2	Preparation	82
6.14.2.3	Activities	82
6.14.2.4	Verdict.....	82
6.14.2.5	Evidence.....	83
6.14.2.6	Guidance	83
6.15	Factory reset and data portability	83
6.15.1	Overview	83
6.15.2	REQ-SDT-01 Secure deletion.....	83
6.15.2.1	Objective	83
6.15.2.2	Preparation	83
6.15.2.3	Activities	83
6.15.2.4	Verdict.....	84
6.15.2.5	Evidence.....	84
6.15.2.6	Guidance	84
6.15.3	REQ-SDT-02 Secure data read provided by operational environment.....	84
6.15.3.1	Objective	84
6.15.3.2	Preparation	84
6.15.3.3	Activities	84
6.15.3.4	Verdict.....	84
6.15.3.5	Evidence.....	85
Annex A (informative):	Relationship between the present document and the essential cybersecurity requirements of EU Regulation (EU) 2024/2847.....	86
Annex B (informative):	Security analysis.....	89
B.0	Overview	89
B.1	Assets	89
B.1.1	Data	89
B.1.2	Product functions.....	89
B.1.2.1	Physical network interface essential functions.....	89
B.1.2.2	Device driver essential functions	90
B.1.2.3	Virtual network interface essential functions.....	90
B.1.3	Hardware	91
B.2	Risk factors.....	91
B.2.1	List of risk factors.....	91
B.2.2	[RF-PHY] Physical access to product	91
B.2.3	[RF-NET] Access to attached network.....	91
B.2.4	[RF-COM] Complexity of product functions.....	91
B.2.5	[RF-HOS] Impact of access to host system assets.....	92
B.2.6	[RF-FUN] Sensitivity of functions of product	92
B.2.7	[RF-ADM] Availability and skill of administration	92
B.2.8	[RF-INI] Operational environment of initial setup.....	93
B.3	Assumptions	93
B.3.1	Overview	93
B.3.2	Proper host system.....	93
B.3.3	Proper administrator.....	93
B.3.4	Attacker has limited physical access to product.....	93

B.3.5	Attacker has limited resources.....	93
B.4	Threats and security analysis of threats.....	93
B.4.1	General	93
B.4.2	Security analysis methodology.....	94
B.4.3	List of threats, risk assessments, and mitigations	94
B.4.3.1	TH-UEVU: Unknown exploitable vulnerabilities	94
B.4.3.2	TH-KEVU: Known exploitable vulnerabilities	95
B.4.3.3	TH-DSTP: Compromise of data stored on product.....	95
B.4.3.4	TH-CONF: Access to assets via configuration errors.....	96
B.4.3.5	TH-UADT: Unauthorized access to data transmitted	97
B.4.3.6	TH-AVAI: Denial of service attack on product.....	98
B.4.3.7	TH-DDOS: Interference with other devices	99
B.5	Mapping of use cases to risk factors	100
B.6	Mapping of threats to requirements.....	100
B.7	Risks not treated by the requirements	100

Annexes C to

J:	Void
.....	101

Annex K (normative): Generic cryptographic requirements and assessment.....102

K.1	Cryptography.....	102
K.1.1	Requirement	102
K.1.2	Assessment of product cryptographic configuration	102
K.1.2.1	General.....	102
K.1.2.2	Assessment of ACM-listed cryptographic mechanisms.....	103
K.1.2.2.1	Assessment objective	103
K.1.2.2.2	Assessment preparation.....	103
K.1.2.2.3	Assessment activities	103
K.1.2.2.4	Assessment evidence.....	103
K.1.2.2.5	Assessment verdict.....	103
K.1.2.3	Assessment of ACM-extended cryptographic mechanisms.....	104
K.1.2.3.1	Assessment objective	104
K.1.2.3.2	Assessment preparation.....	104
K.1.2.3.3	Assessment activities	104
K.1.2.3.4	Assessment evidence.....	104
K.1.2.3.5	Assessment verdict.....	105
K.1.2.4	Assessment of interoperability-based cryptographic mechanisms.....	105
K.1.2.4.1	Assessment objective	105
K.1.2.4.2	Assessment preparation.....	105
K.1.2.4.3	Assessment activities	105
K.1.2.4.4	Assessment evidence.....	105
K.1.2.4.5	Assessment verdict.....	106
K.2	Crypto agility.....	106
K.2.1	Requirement	106
K.2.2	Assessment of crypto-agility	106
K.2.2.1	Assessment objective.....	106
K.2.2.2	Assessment preparation	106
K.2.2.3	Assessment activities	107
K.2.2.4	Assessment evidence	107
K.2.2.5	Assessment verdict	107
K.3	ACM-extended cryptographic mechanisms	107
K.3.1	Requirement	107
K.3.2	List of ACM-extended cryptographic mechanisms.....	108
K.3.3	Assessment.....	112
K.4	Interoperability-based cryptographic mechanisms.....	112
K.4.1	Requirement	112

K.4.2	List of interoperability-based cryptographic mechanisms	113
K.4.3	Assessment	114

Annexes L to

Q:	Void
.....	115

Annex R (normative): Remote Data Processing Solutions116

R.1	Scope & Applicability	116
R.2	RDPS as a product-boundary extension	116
R.3	Threat Model	117
R.3.1	Introduction	117
R.3.2	Assets	117
R.3.3	Threat catalogue	118
R.3.3.1	Overview	118
R.3.3.2	T-RDPS-01 Loss of data authenticity of interactions across the RDPS boundary	118
R.3.3.3	T-RDPS-02 Loss of integrity of interactions across the RDPS boundary	118
R.3.3.4	T-RDPS-03 Unauthorized disclosure of interactions across the RDPS boundary	119
R.3.3.5	T-RDPS-04 Degradation of interactions across the RDPS boundary	119
R.3.4	Assets to Threats mapping	119
R.4	Security Requirements	119
R.4.1	General and guidance for requirement-structure selection	119
R.4.2	Applicability of Annex R requirements	120
R.4.3	Local product side requirements	121
R.4.3.1	REQ-RDPS-L-AUTH-001	121
R.4.3.2	REQ-RDPS-L-AUTH-002	121
R.4.3.3	REQ-RDPS-L-AUTH-003	121
R.4.3.4	REQ-RDPS-L-INTEG-001	121
R.4.3.5	REQ-RDPS-L-INTEG-002	122
R.4.3.6	REQ-RDPS-L-INTEG-003	122
R.4.3.7	REQ-RDPS-L-CONF-001	122
R.4.3.8	REQ-RDPS-L-CONF-002	122
R.4.3.9	REQ-RDPS-L-CONF-003	123
R.4.3.10	REQ-RDPS-L-AVAIL-001	123
R.4.3.11	REQ-RDPS-L-AVAIL-002	123
R.4.3.12	REQ-RDPS-L-AVAIL-003	124
R.4.4	RDPS side requirements	124
R.4.4.1	REQ-RDPS-R-AUTH-001	124
R.4.4.2	REQ-RDPS-R-AUTH-002	124
R.4.4.3	REQ-RDPS-R-AUTH-003	124
R.4.4.4	REQ-RDPS-R-INTEG-001	125
R.4.4.5	REQ-RDPS-R-INTEG-002	125
R.4.4.6	REQ-RDPS-R-INTEG-003	125
R.4.4.7	REQ-RDPS-R-CONF-001	125
R.4.4.8	REQ-RDPS-R-CONF-002	126
R.4.4.9	REQ-RDPS-R-CONF-003	126
R.4.4.10	REQ-RDPS-R-AVAIL-001	126
R.4.4.11	REQ-RDPS-R-AVAIL-002	126
R.4.4.12	REQ-RDPS-R-AVAIL-003	127
R.4.5	Threats ↔ Requirements mapping	127
R.5	Conformity assessment	128
R.5.1	Overview	128
R.5.2	Applicability	128
R.5.3	Local product side requirements	128
R.5.3.1	Assessment case for REQ-RDPS-L-AUTH-001	128
R.5.3.1.1	Objective	128
R.5.3.1.2	Preparation	128
R.5.3.1.3	Activities	128
R.5.3.1.4	Verdict	128

R.5.3.1.5	Evidence.....	129
R.5.3.2	Assessment case for REQ-RDPS-L-AUTH-002	129
R.5.3.2.1	Objective	129
R.5.3.2.2	Preparation	129
R.5.3.2.3	Activities	129
R.5.3.2.4	Verdict.....	129
R.5.3.2.5	Evidence.....	130
R.5.3.3	Assessment case for REQ-RDPS-L-AUTH-003	130
R.5.3.3.1	Objective	130
R.5.3.3.2	Preparation	130
R.5.3.3.3	Activities	130
R.5.3.3.4	Verdict.....	130
R.5.3.3.5	Evidence.....	131
R.5.3.4	Assessment case for REQ-RDPS-L-INTEG-001.....	131
R.5.3.4.1	Objective	131
R.5.3.4.2	Preparation	131
R.5.3.4.3	Activities	131
R.5.3.4.4	Verdict.....	131
R.5.3.4.5	Evidence.....	131
R.5.3.5	Assessment case for REQ-RDPS-L-INTEG-002.....	132
R.5.3.5.1	Objective	132
R.5.3.5.2	Preparation	132
R.5.3.5.3	Activities	132
R.5.3.5.4	Verdict.....	132
R.5.3.5.5	Evidence.....	132
R.5.3.6	Assessment case for REQ-RDPS-L-INTEG-003.....	133
R.5.3.6.1	Objective	133
R.5.3.6.2	Preparation	133
R.5.3.6.3	Activities	133
R.5.3.6.4	Verdict.....	133
R.5.3.6.5	Evidence.....	133
R.5.3.7	Assessment case for REQ-RDPS-L-CONF-001	134
R.5.3.7.1	Objective	134
R.5.3.7.2	Preparation	134
R.5.3.7.3	Activities	134
R.5.3.7.4	Verdict.....	134
R.5.3.7.5	Evidence.....	134
R.5.3.8	Assessment case for REQ-RDPS-L-CONF-002	134
R.5.3.8.1	Objective	134
R.5.3.8.2	Preparation	135
R.5.3.8.3	Activities	135
R.5.3.8.4	Verdict.....	135
R.5.3.8.5	Evidence.....	135
R.5.3.9	Assessment case for REQ-RDPS-L-CONF-003	135
R.5.3.9.1	Objective	135
R.5.3.9.2	Preparation	135
R.5.3.9.3	Activities	136
R.5.3.9.4	Verdict.....	136
R.5.3.9.5	Evidence.....	136
R.5.3.10	Assessment case for REQ-RDPS-L-AVAIL-001	136
R.5.3.10.1	Objective	136
R.5.3.10.2	Preparation	136
R.5.3.10.3	Activities	137
R.5.3.10.4	Verdict.....	137
R.5.3.10.5	Evidence.....	137
R.5.3.11	Assessment case for REQ-RDPS-L-AVAIL-002	137
R.5.3.11.1	Objective	137
R.5.3.11.2	Preparation	137
R.5.3.11.3	Activities	137
R.5.3.11.4	Verdict.....	138
R.5.3.11.5	Evidence.....	138
R.5.3.12	Assessment case for REQ-RDPS-L-AVAIL-003	138

R.5.3.12.1	Objective	138
R.5.3.12.2	Preparation	138
R.5.3.12.3	Activities	138
R.5.3.12.4	Verdict	139
R.5.3.12.5	Evidence	139
R.5.4	RDPS side requirements	139
R.5.4.1	Assessment case for REQ-RDPS-R-AUTH-001	139
R.5.4.1.1	Objective	139
R.5.4.1.2	Preparation	139
R.5.4.1.3	Activities	139
R.5.4.1.4	Verdict	140
R.5.4.1.5	Evidence	140
R.5.4.2	Assessment case for REQ-RDPS-R-AUTH-002	140
R.5.4.2.1	Objective	140
R.5.4.2.2	Preparation	140
R.5.4.2.3	Activities	140
R.5.4.2.4	Verdict	141
R.5.4.2.5	Evidence	141
R.5.4.3	Assessment case for REQ-RDPS-R-AUTH-003	141
R.5.4.3.1	Objective	141
R.5.4.3.2	Preparation	141
R.5.4.3.3	Activities	141
R.5.4.3.4	Verdict	142
R.5.4.3.5	Evidence	142
R.5.4.4	Assessment case for REQ-RDPS-R-INTEG-001	142
R.5.4.4.1	Objective	142
R.5.4.4.2	Preparation	142
R.5.4.4.3	Activities	142
R.5.4.4.4	Verdict	142
R.5.4.4.5	Evidence	143
R.5.4.5	Assessment case for REQ-RDPS-R-INTEG-002	143
R.5.4.5.1	Objective	143
R.5.4.5.2	Preparation	143
R.5.4.5.3	Activities	143
R.5.4.5.4	Verdict	143
R.5.4.5.5	Evidence	144
R.5.4.6	Assessment case for REQ-RDPS-R-INTEG-003	144
R.5.4.6.1	Objective	144
R.5.4.6.2	Preparation	144
R.5.4.6.3	Activities	144
R.5.4.6.4	Verdict	144
R.5.4.6.5	Evidence	145
R.5.4.7	Assessment case for REQ-RDPS-R-CONF-001	145
R.5.4.7.1	Objective	145
R.5.4.7.2	Preparation	145
R.5.4.7.3	Activities	145
R.5.4.7.4	Verdict	145
R.5.4.7.5	Evidence	145
R.5.4.8	Assessment case for REQ-RDPS-R-CONF-002	146
R.5.4.8.1	Objective	146
R.5.4.8.2	Preparation	146
R.5.4.8.3	Activities	146
R.5.4.8.4	Verdict	146
R.5.4.8.5	Evidence	146
R.5.4.9	Assessment case for REQ-RDPS-R-CONF-003	146
R.5.4.9.1	Objective	146
R.5.4.9.2	Preparation	146
R.5.4.9.3	Activities	147
R.5.4.9.4	Verdict	147
R.5.4.9.5	Evidence	147
R.5.4.10	Assessment case for REQ-RDPS-R-AVAIL-001	147
R.5.4.10.1	Objective	147

R.5.4.10.2	Preparation.....	147
R.5.4.10.3	Activities	148
R.5.4.10.4	Verdict	148
R.5.4.10.5	Evidence	148
R.5.4.11	Assessment case for REQ-RDPS-R-AVAIL-002	148
R.5.4.11.1	Objective	148
R.5.4.11.2	Preparation.....	148
R.5.4.11.3	Activities	149
R.5.4.11.4	Verdict	149
R.5.4.11.5	Evidence	149
R.5.4.12	Assessment case for REQ-RDPS-R-AVAIL-003	149
R.5.4.12.1	Objective	149
R.5.4.12.2	Preparation.....	149
R.5.4.12.3	Activities	149
R.5.4.12.4	Verdict	150
R.5.4.12.5	Evidence	150
R.5.5	Assessment cases for mono-level alternative proposals	150
R.5.5.1	Assessment case for REQ-RDPS-L-AUTH-001.....	150
R.5.5.1.1	Objective	150
R.5.5.1.2	Preparation.....	150
R.5.5.1.3	Activities	150
R.5.5.1.4	Verdict	151
R.5.5.1.5	Evidence	151
R.5.5.2	Assessment case for REQ-RDPS-L-INTEG-001	151
R.5.5.2.1	Objective	151
R.5.5.2.2	Preparation.....	151
R.5.5.2.3	Activities	151
R.5.5.2.4	Verdict	152
R.5.5.2.5	Evidence	152
R.5.5.3	Assessment case for REQ-RDPS-L-CONF-001	152
R.5.5.3.1	Objective	152
R.5.5.3.2	Preparation.....	152
R.5.5.3.3	Activities	152
R.5.5.3.4	Verdict	152
R.5.5.3.5	Evidence	153
R.5.5.4	Assessment case for REQ-RDPS-L-AVAIL-001	153
R.5.5.4.1	Objective	153
R.5.5.4.2	Preparation.....	153
R.5.5.4.3	Activities	153
R.5.5.4.4	Verdict	153
R.5.5.4.5	Evidence	154
R.5.5.5	Assessment case for REQ-RDPS-R-AUTH-001.....	154
R.5.5.5.1	Objective	154
R.5.5.5.2	Preparation.....	154
R.5.5.5.3	Activities	154
R.5.5.5.4	Verdict	154
R.5.5.5.5	Evidence	155
R.5.5.6	Assessment case for REQ-RDPS-R-INTEG-001.....	155
R.5.5.6.1	Objective	155
R.5.5.6.2	Preparation.....	155
R.5.5.6.3	Activities	155
R.5.5.6.4	Verdict	155
R.5.5.6.5	Evidence	155
R.5.5.7	Assessment case for REQ-RDPS-R-CONF-001	156
R.5.5.7.1	Objective	156
R.5.5.7.2	Preparation.....	156
R.5.5.7.3	Activities	156
R.5.5.7.4	Verdict	156
R.5.5.7.5	Evidence	156
R.5.5.8	Assessment case for REQ-RDPS-R-AVAIL-001	156
R.5.5.8.1	Objective	156
R.5.5.8.2	Preparation.....	157

R.5.5.8.3	Activities	157
R.5.5.8.4	Verdict	157
R.5.5.8.5	Evidence	157
R.6	Mapping of CRA Annex I to Annex R requirements	157
History		160

Sample Document

get full document from standards.iteh.ai

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)) may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential; or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the [ETSI IPR online database](#).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are; or may be; or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

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) 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