



**Cyber Security (CYBER);
CRA;
Cybersecurity requirements
for Virtualisation Execution Stack (VES)
and Container Execution Stack (CES),
including hypervisors and container runtime systems**

Reference

DEN/CYBER-EUS-0016

Keywords

container, CRA, cybersecurity, virtualisation

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	13
Foreword.....	13
Modal verbs terminology.....	14
Introduction	14
1 Scope	15
2 References	15
2.1 Normative references	15
2.2 Informative references.....	16
3 Definition of terms, symbols and abbreviations.....	17
3.1 Terms.....	17
3.2 Symbols.....	19
3.3 Abbreviations	19
4 Product Context.....	21
4.1 Product Functions.....	21
4.1.1 General.....	21
4.1.2 VES.....	21
4.1.2.1 Intended purpose and reasonably foreseeable use of the VES	21
4.1.2.2 Intended purpose and reasonably foreseeable use of the Hypervisor.....	21
4.1.2.3 Intended purpose and reasonably foreseeable use of the M&O system	22
4.1.3 CES.....	22
4.1.3.1 Intended purpose and reasonably foreseeable use of the CES	22
4.1.3.2 Intended purpose and reasonably foreseeable use of the CRS	22
4.1.3.3 Intended purpose and reasonably foreseeable use of the CE.....	23
4.1.3.4 Intended purpose and reasonably foreseeable use of the CO	23
4.2 Product architecture.....	23
4.2.1 General distinction of components	23
4.2.2 VES.....	23
4.2.2.1 Architectural types and virtualisation techniques of VES.....	23
4.2.2.2 In-scope components of the VES	24
4.2.2.2.1 Hypervisor	24
4.2.2.2.2 Management and Orchestration System	25
4.2.2.3 Security-relevant environmental dependencies (out of scope).....	26
4.2.3 CES	27
4.2.3.1 In-scope components.....	27
4.2.3.2 Security-relevant environmental dependencies (out of scope).....	28
4.2.4 Deployment of M&O, CE, and CO outside the local execution environment	28
4.2.5 Product variants and conforming products	29
4.2.5.1 Definition of conforming products.....	29
4.2.5.2 Product variants.....	29
4.3 Operational environment.....	30
4.3.1 General Principles.....	30
4.3.2 Security Objectives for the Operational Environment	30
4.3.3 Reference to Relevant CRA Harmonised Standards.....	32
4.4 Distribution of Security Functions	32
4.5 Users.....	32
4.6 Use cases	33
4.6.1 Purpose	33
4.6.2 Use Cases for VES.....	33
4.6.3 Use Cases for CES.....	35
4.6.4 Use Case to Risk Mapping.....	37
5 Technical Requirements for products.....	37
5.1 Risk-Based requirement classes/categorization and application	37
5.1.1 Requirement Classes, Categorization and Security Profiles	37

5.1.1.1	Definition of Requirement Classes: Basic, Elevated, Advanced.....	37
5.1.1.2	Security Profile Definitions.....	38
5.1.1.3	Requirement Categorization.....	38
5.1.1.4	Guidance for Manufacturers.....	39
5.1.2	Requirement Application.....	40
5.1.2.1	Approaches for determining security requirements	40
5.1.2.2	SP-Based Requirement Application.....	40
5.1.3	Applicability of requirements	41
5.2	VES Security Requirements	42
5.2.1	Hypervisor Requirements	42
5.2.1.1	Isolation.....	42
5.2.1.1.1	General	42
5.2.1.1.2	VM Isolation.....	42
5.2.1.1.3	Control Plane Isolation	43
5.2.1.1.4	Network Plane Separation	44
5.2.1.2	Integrity Protection.....	45
5.2.1.2.1	Boot integrity verification	45
5.2.1.2.2	Guest VM image integrity verification.....	46
5.2.1.2.3	Runtime integrity protection.....	47
5.2.1.2.4	Remote attestation	47
5.2.1.3	Authentication.....	48
5.2.1.3.1	General	48
5.2.1.3.2	Administrative Authentication	49
5.2.1.3.3	Service Authentication	49
5.2.1.4	Authorization	50
5.2.1.4.1	General	50
5.2.1.4.2	Administrative Authorization	50
5.2.1.4.3	Service Authorization.....	51
5.2.1.5	Confidentiality Protection	51
5.2.1.6	Availability and Resilience	52
5.2.1.7	Logging	53
5.2.1.8	Secure Update	54
5.2.1.9	Secure Configuration and Default.....	55
5.2.1.10	Data Minimisation.....	56
5.2.1.11	Decommissioning.....	56
5.2.2	Management and Orchestration System Requirements	57
5.2.2.1	General applicability	57
5.2.2.2	Authentication.....	57
5.2.2.3	Authorization	57
5.2.2.4	Secure Configuration	58
5.2.2.5	Communication Security.....	58
5.2.2.6	Integrity Protection.....	59
5.2.2.7	Logging	59
5.2.2.8	Secure Update	60
5.2.2.9	Decommissioning and Secure Transfer.....	61
5.3	CES Security Requirements	61
5.3.1	CRS Requirements.....	61
5.3.1.1	Isolation.....	61
5.3.1.1.1	Container Isolation	61
5.3.1.1.2	Control Plane Isolation	62
5.3.1.1.3	Network Plane Isolation	62
5.3.1.2	Integrity Protection.....	63
5.3.1.2.1	Boot integrity verification	63
5.3.1.2.2	Container image integrity verification.....	64
5.3.1.2.3	Runtime integrity protection.....	65
5.3.1.2.4	Remote attestation	65
5.3.1.3	Authentication.....	66
5.3.1.3.1	General	66
5.3.1.3.2	Administrative Authentication	67
5.3.1.3.3	Service Authentication	67
5.3.1.4	Authorization	68
5.3.1.4.1	General	68

5.3.1.4.2	Administrative Authorization	68
5.3.1.4.3	Service Authorization	69
5.3.1.5	Confidentiality Protection	69
5.3.1.6	Availability and Resilience	70
5.3.1.7	Logging	71
5.3.1.8	Secure Update	72
5.3.1.9	Secure Configuration and Default	73
5.3.1.10	Data Minimisation	73
5.3.1.11	Decommissioning	74
5.3.2	CE Requirements	74
5.3.2.1	Isolation	74
5.3.2.2	Integrity Protection	74
5.3.2.3	Authentication	75
5.3.2.4	Authorization	75
5.3.2.5	Confidentiality	76
5.3.2.6	Secure Update	76
5.3.2.7	Decommissioning and secure data deletion	77
5.3.3	CO Requirements	78
5.3.3.1	Isolation	78
5.3.3.2	Integrity Protection	78
5.3.3.3	Authentication	78
5.3.3.4	Authorization	79
5.3.3.5	Confidentiality	79
5.3.3.6	Secure Update	80
5.3.3.7	Decommissioning and secure data deletion	81
5.4	Assurance Security Requirements	81
5.4.1	Vulnerability Management	81
5.4.2	Software Bill of Materials (SBOM)	82
6	Assessment criteria for compliance with technical requirements	83
6.1	Assessment Methodology	83
6.1.1	General Assessment Procedure	83
6.1.2	Technology-neutral Assessment	84
6.1.2.1	General	84
6.1.2.2	Equivalence of Hardware-based and Software-based Approaches	85
6.1.2.3	Technology-neutral Assessment Principles	86
6.1.3	Assessment of RDPS requirements	87
6.2	Assessment Report Requirements	87
6.2.1	Mandatory Report Contents	87
6.2.2	Traceability Requirements	89
6.2.3	Evidence Package	89
6.3	VES	90
6.3.1	Hypervisor	90
6.3.1.1	Assessment for VM Isolation	90
6.3.1.1.1	Assessment Case AC-H-VM-ISO-001	90
6.3.1.1.2	Assessment Case AC-H-VM-ISO-002	91
6.3.1.1.3	Assessment Case AC-H-VM-ISO-003	92
6.3.1.1.4	Assessment Case AC-H-VM-ISO-004	94
6.3.1.2	Assessment for Control Plane Isolation	95
6.3.1.2.1	Assessment Case AC-H-CP-ISO-001	95
6.3.1.2.2	Assessment Case AC-H-CP-ISO-002	96
6.3.1.2.3	Assessment Case AC-H-CP-ISO-003	97
6.3.1.3	Assessment for Network Plane Separation	99
6.3.1.3.1	Assessment Case AC-H-NP-ISO-001	99
6.3.1.3.2	Assessment Case AC-H-NP-ISO-002	100
6.3.1.3.3	Assessment Case AC-H-NP-ISO-003	101
6.3.1.4	Assessment for Boot Integrity Verification	102
6.3.1.4.1	Assessment Case AC-H-B-INT-002	102
6.3.1.5	Assessment for Guest VM Image Integrity Verification	104
6.3.1.5.1	Assessment Case AC-H-IMG-INT-001	104
6.3.1.5.2	Assessment Case AC-H-IMG-INT-002	105
6.3.1.5.3	Assessment Case AC-H-IMG-INT-003	107

6.3.1.6	Assessment for Runtime Integrity Protection	108
6.3.1.6.1	Assessment Case AC-H-RP-INT-002	108
6.3.1.7	Assessment for Remote Attestation	109
6.3.1.7.1	Assessment Case AC-H-RA-INT-003.....	109
6.3.1.7.2	Assessment Case AC-H-RA-INT-004.....	111
6.3.1.8	Assessment for Administrative Authentication.....	113
6.3.1.8.1	Assessment Case AC-H-ADMIN-AUTH-001	113
6.3.1.8.2	Assessment Case AC-H-ADMIN-AUTH-002	114
6.3.1.8.3	Assessment Case AC-H-ADMIN-AUTH-003	115
6.3.1.9	Assessment for Service Authentication.....	116
6.3.1.9.1	Assessment Case AC-H-SERV-AUTH-001.....	116
6.3.1.9.2	Assessment Case AC-H-SERV-AUTH-002.....	117
6.3.1.9.3	Assessment Case AC-H-SERV-AUTH-003.....	118
6.3.1.10	Assessment for Administrative Authorization	119
6.3.1.10.1	Assessment Case AC-H-ADMIN-AUTHZ-001.....	119
6.3.1.10.2	Assessment Case AC-H-ADMIN-AUTHZ-002.....	120
6.3.1.10.3	Assessment Case AC-H-ADMIN-AUTHZ-003.....	121
6.3.1.11	Assessment for Service Authorization	122
6.3.1.11.1	Assessment Case AC-H-SERV-AUTHZ-001	122
6.3.1.11.2	Assessment Case AC-H-SERV-AUTHZ-002	123
6.3.1.11.3	Assessment Case AC-H-SERV-AUTHZ-003	124
6.3.1.12	Assessment for Confidentiality Protection.....	125
6.3.1.12.1	Assessment Case AC-H-CONF-001.....	125
6.3.1.12.2	Assessment Case AC-H-CONF-002.....	126
6.3.1.12.3	Assessment Case AC-H-CONF-003.....	128
6.3.1.12.4	Assessment Case AC-H-CONF-004.....	129
6.3.1.13	Assessment for Availability and Resilience	130
6.3.1.13.1	Assessment Case AC-H-AVAIL-001	130
6.3.1.13.2	Assessment Case AC-H-AVAIL-002	131
6.3.1.13.3	Assessment Case AC-H-AVAIL-003	132
6.3.1.14	Assessment for Logging.....	134
6.3.1.14.1	Assessment Case AC-H-LOG-001	134
6.3.1.14.2	Assessment Case AC-H-LOG-002	134
6.3.1.14.3	Assessment Case AC-H-LOG-003	135
6.3.1.15	Assessment for Secure Update.....	137
6.3.1.15.1	Assessment Case AC-H-UPD-001	137
6.3.1.15.2	Assessment Case AC-H-UPD-002	139
6.3.1.15.3	Assessment Case AC-H-UPD-003	140
6.3.1.16	Assessment for Secure Configuration and Default	142
6.3.1.16.1	Assessment Case AC-H-CFG-001	142
6.3.1.16.2	Assessment Case AC-H-CFG-002	143
6.3.1.16.3	Assessment Case AC-H-CFG-003	144
6.3.1.17	Assessment for Data Minimisation	145
6.3.1.17.1	Assessment Case AC-H-DM-001.....	145
6.3.1.17.2	Assessment Case AC-H-DM-002.....	146
6.3.1.18	Assessment for Decommissioning	147
6.3.1.18.1	Assessment Case AC-H-DECOM-001.....	147
6.3.2	M&O System	148
6.3.2.1	Assessment for Authentication.....	148
6.3.2.1.1	Assessment Case AC-M&O-AUTH-001	148
6.3.2.1.2	Assessment Case AC-M&O-AUTH-002	149
6.3.2.1.3	Assessment Case AC-M&O-AUTH-003	150
6.3.2.2	Assessment for Authorization	151
6.3.2.2.1	Assessment Case AC-M&O-AUTHZ-001	151
6.3.2.2.2	Assessment Case AC-M&O-AUTHZ-002	152
6.3.2.2.3	Assessment Case AC-M&O-AUTHZ-003	153
6.3.2.3	Assessment for Secure Configuration	154
6.3.2.3.1	Assessment Case AC-M&O-CFG-001.....	154
6.3.2.3.2	Assessment Case AC-M&O-CFG-002.....	155
6.3.2.3.3	Assessment Case AC-M&O-CFG-003.....	155
6.3.2.4	Assessment for Communication Security	156
6.3.2.4.1	Assessment Case AC-M&O-COM-001	156

6.3.2.4.2	Assessment Case AC-M&O-COM-002	157
6.3.2.4.3	Assessment Case AC-M&O-COM-003	158
6.3.2.5	Assessment for Integrity Protection	159
6.3.2.5.1	Assessment Case AC-M&O-INT-001	159
6.3.2.5.2	Assessment Case AC-M&O-INT-002	160
6.3.2.5.3	Assessment Case AC-M&O-INT-003	161
6.3.2.6	Assessment for Logging	162
6.3.2.6.1	Assessment Case AC-M&O-LOG-001	162
6.3.2.6.2	Assessment Case AC-M&O-LOG-002	162
6.3.2.6.3	Assessment Case AC-M&O-LOG-003	163
6.3.2.7	Assessment for Secure Update	164
6.3.2.7.1	Assessment Case AC-M&O-UPD-001	164
6.3.2.7.2	Assessment Case AC-M&O-UPD-002	166
6.3.2.7.3	Assessment Case AC-M&O-UPD-003	168
6.3.2.8	Assessment for Decommissioning and Secure Transfer	169
6.3.2.8.1	Assessment Case AC-M&O-DECOM-001	169
6.3.2.8.2	Assessment Case AC-M&O-DECOM-002	170
6.4	CES	171
6.4.1	CRS	171
6.4.1.1	Assessment for Container Isolation	171
6.4.1.1.1	Assessment Case AC-CRS-CN-ISO-001	171
6.4.1.1.2	Assessment Case AC-CRS-CN-ISO-002	172
6.4.1.1.3	Assessment Case AC-CRS-CN-ISO-003	174
6.4.1.2	Assessment for Control Plane Isolation	175
6.4.1.2.1	Assessment Case AC-CRS-CP-ISO-001	175
6.4.1.2.2	Assessment Case AC-CRS-CP-ISO-002	176
6.4.1.2.3	Assessment Case AC-CRS-CP-ISO-003	177
6.4.1.3	Assessment for Network Plane Isolation	179
6.4.1.3.1	Assessment Case AC-CRS-NP-ISO-001	179
6.4.1.3.2	Assessment Case AC-CRS-NP-ISO-002	180
6.4.1.3.3	Assessment Case AC-CRS-NP-ISO-003	181
6.4.1.4	Assessment for Boot Integrity Verification	183
6.4.1.4.1	Assessment Case AC-CRS-B-INT-002	183
6.4.1.5	Assessment for Container Image Integrity Verification	185
6.4.1.5.1	Assessment Case AC-CRS-IMG-INT-001	185
6.4.1.5.2	Assessment Case AC-CRS-IMG-INT-002	186
6.4.1.5.3	Assessment Case AC-CRS-IMG-INT-003	187
6.4.1.6	Assessment for Runtime Integrity Protection	189
6.4.1.6.1	Assessment Case AC-CRS-RP-INT-002	189
6.4.1.7	Assessment for Remote Attestation	190
6.4.1.7.1	Assessment Case AC-CRS-RA-INT-003	190
6.4.1.7.2	Assessment Case AC-CRS-RA-INT-004	192
6.4.1.8	Assessment for Administrative Authentication	194
6.4.1.8.1	Assessment Case AC-CRS-ADMIN-AUTH-001	194
6.4.1.8.2	Assessment Case AC-CRS-ADMIN-AUTH-002	195
6.4.1.8.3	Assessment Case AC-CRS-ADMIN-AUTH-003	196
6.4.1.9	Assessment for Service Authentication	197
6.4.1.9.1	Assessment Case AC-CRS-SERV-AUTH-001	197
6.4.1.9.2	Assessment Case AC-CRS-SERV-AUTH-002	198
6.4.1.9.3	Assessment Case AC-CRS-SERV-AUTH-003	199
6.4.1.10	Assessment for Administrative Authorization	200
6.4.1.10.1	Assessment Case AC-CRS-ADMIN-AUTHZ-001	200
6.4.1.10.2	Assessment Case AC-CRS-ADMIN-AUTHZ-002	201
6.4.1.10.3	Assessment Case AC-CRS-ADMIN-AUTHZ-003	202
6.4.1.11	Assessment for Service Authorization	203
6.4.1.11.1	Assessment Case AC-CRS-SERV-AUTHZ-001	203
6.4.1.11.2	Assessment Case AC-CRS-SERV-AUTHZ-002	204
6.4.1.11.3	Assessment Case AC-CRS-SERV-AUTHZ-003	205
6.4.1.12	Assessment for Confidentiality Protection	206
6.4.1.12.1	Assessment Case AC-CRS-CONF-001	206
6.4.1.12.2	Assessment Case AC-CRS-CONF-002	208
6.4.1.12.3	Assessment Case AC-CRS-CONF-003	209

6.4.1.12.4	Assessment Case AC-CRS-CONF-004	211
6.4.1.13	Assessment for Availability and Resilience	213
6.4.1.13.1	Assessment Case AC-CRS-AVAIL-001	213
6.4.1.13.2	Assessment Case AC-CRS-AVAIL-002	214
6.4.1.13.3	Assessment Case AC-CRS-AVAIL-003	215
6.4.1.13.4	Assessment Case AC-CRS-AVAIL-004	216
6.4.1.14	Assessment for Logging	217
6.4.1.14.1	Assessment Case AC-CRS-LOG-001	217
6.4.1.14.2	Assessment Case AC-CRS-LOG-002	218
6.4.1.14.3	Assessment Case AC-CRS-LOG-003	219
6.4.1.15	Assessment for Secure Update	220
6.4.1.15.1	Assessment Case AC-CRS-UPD-001	220
6.4.1.15.2	Assessment Case AC-CRS-UPD-002	222
6.4.1.15.3	Assessment Case AC-CRS-UPD-003	224
6.4.1.16	Assessment for Secure Configuration and Default	225
6.4.1.16.1	Assessment Case AC-CRS-CFG-001	225
6.4.1.16.2	Assessment Case AC-CRS-CFG-002	226
6.4.1.16.3	Assessment Case AC-CRS-CFG-003	227
6.4.1.17	Assessment for Data Minimisation	228
6.4.1.17.1	Assessment Case AC-CRS-DM-001	228
6.4.1.17.2	Assessment Case AC-CRS-DM-002	229
6.4.1.18	Assessment for Decommissioning	230
6.4.1.18.1	Assessment Case AC-CRS-DECOM-001	230
6.4.2	CE	231
6.4.2.1	Assessment for Isolation	231
6.4.2.1.1	Assessment Case AC-CE-ISO-001	231
6.4.2.1.2	Assessment Case AC-CE-ISO-002	232
6.4.2.1.3	Assessment Case AC-CE-ISO-003	233
6.4.2.2	Assessment for Integrity Protection	234
6.4.2.2.1	Assessment Case AC-CE-INTEG-001	234
6.4.2.2.2	Assessment Case AC-CE-INTEG-002	235
6.4.2.2.3	Assessment Case AC-CE-INTEG-003	236
6.4.2.3	Assessment for Authentication	237
6.4.2.3.1	Assessment Case AC-CE-AUTH-001	237
6.4.2.3.2	Assessment Case AC-CE-AUTH-002	238
6.4.2.3.3	Assessment Case AC-CE-AUTH-003	238
6.4.2.4	Assessment for Authorization	239
6.4.2.4.1	Assessment Case AC-CE-AUTHZ-001	239
6.4.2.4.2	Assessment Case AC-CE-AUTHZ-002	240
6.4.2.4.3	Assessment Case AC-CE-AUTHZ-003	241
6.4.2.5	Assessment for Confidentiality and Data Protection	242
6.4.2.5.1	Assessment Case AC-CE-CONF-001	242
6.4.2.5.2	Assessment Case AC-CE-CONF-002	243
6.4.2.5.3	Assessment Case AC-CE-CONF-003	243
6.4.2.6	Assessment for Secure Update	245
6.4.2.6.1	Assessment Case AC-CE-UPD-001	245
6.4.2.6.2	Assessment Case AC-CE-UPD-002	247
6.4.2.7	Assessment for Decommissioning and Secure Transfer	248
6.4.2.7.1	Assessment Case AC-CE-DECOM-001	248
6.4.2.7.2	Assessment Case AC-CE-DECOM-002	249
6.4.3	CO	250
6.4.3.1	Assessment for Isolation	250
6.4.3.1.1	Assessment Case AC-CO-ISO-001	250
6.4.3.1.2	Assessment Case AC-CO-ISO-002	251
6.4.3.1.3	Assessment Case AC-CO-ISO-003	252
6.4.3.2	Assessment for Integrity Protection	252
6.4.3.2.1	Assessment Case AC-CO-INTEG-001	252
6.4.3.2.2	Assessment Case AC-CO-INTEG-002	253
6.4.3.2.3	Assessment Case AC-CO-INTEG-003	254
6.4.3.3	Assessment for Authentication	255
6.4.3.3.1	Assessment Case AC-CO-AUTH-001	255
6.4.3.3.2	Assessment Case AC-CO-AUTH-002	256

6.4.3.3.3	Assessment Case AC-CO-AUTH-003	256
6.4.3.4	Assessment for Authorization	257
6.4.3.4.1	Assessment Case AC-CO-AUTHZ-001	257
6.4.3.4.2	Assessment Case AC-CO-AUTHZ-002	258
6.4.3.4.3	Assessment Case AC-CO-AUTHZ-003	259
6.4.3.5	Assessment for Confidentiality and Data Protection.....	260
6.4.3.5.1	Assessment Case AC-CO-CONF-001	260
6.4.3.5.2	Assessment Case AC-CO-CONF-002	261
6.4.3.5.3	Assessment Case AC-CO-CONF-003	261
6.4.3.6	Assessment for Secure Update	262
6.4.3.6.1	Assessment Case AC-CO-UPD-001.....	262
6.4.3.6.2	Assessment Case AC-CO-UPD-002.....	264
6.4.3.6.3	Assessment Case AC-CO-UPD-003.....	266
6.4.3.7	Assessment for Decommissioning and Secure Transfer	267
6.4.3.7.1	Assessment Case AC-CO-DECOM-001	267
6.4.3.7.2	Assessment Case AC-CO-DECOM-002	268
6.5	Assessment for Assurance Security Requirements.....	269
6.5.1	Assessment for Vulnerability Management	269
6.5.1.1	Assessment Case AC-ASSUR-VULM-001	269
6.5.2	Assessment for Software Bill of Materials (SBOM)	270
6.5.2.1	Assessment Case AC-ASSUR-SBOM-001.....	270
6.5.2.2	Assessment Case AC-ASSUR-SBOM-002.....	271
6.5.2.3	Assessment Case AC-ASSUR-SBOM-003.....	273

Annex A (informative):	Relationship between the present document and the requirements of EU Regulation (EU) 2024/2847 - the Cyber Resilience Act.....	274
-------------------------------	---	------------

Annex B (informative):	Security Analysis.....	278
-------------------------------	-------------------------------	------------

B.1	Overview	278
B.2	Threats	278
B.2.1	Overview	278
B.2.2	VES	279
B.2.2.1	Hyper Type I.....	279
B.2.2.2	Hyper Type II	280
B.2.2.3	Orchestration and Management system	281
B.2.3	CES	282
B.2.3.1	Container Orchestrator.....	282
B.2.3.2	Container Engine	284
B.2.3.3	Container Runtime System	285
B.2.4	Hardware-level common threat	286
B.3	Risk Assessment Process.....	286
B.4	Risk Factor Scoring.....	287
B.5	Calculation and Mapping to Likelihood/Impact Levels.....	290
B.5.1	General	290
B.5.2	Likelihood Score	290
B.5.3	Impact Score.....	290
B.6	Risk Matrix.....	291
B.7	Risk Methodology Applied to Use Cases.....	291
B.7.1	General	291
B.7.2	Risk Evaluation of VES use cases.....	292
B.7.2.1	Hypervisor Type I.....	292
B.7.2.2	Hypervisor Type II.....	296
B.7.2.3	M&O System.....	300
B.7.3	Risk Evaluation of CES use cases	304
B.7.3.1	CRS.....	304
B.7.3.2	CE	309
B.7.3.3	CO.....	313

B.7.4	Risk Evaluation of common hardware-level threat T-ALL-HW-ACCESS.....	318
B.8	Threat-to-Requirement Traceability Matrix	321
B.8.1	VES	321
B.8.1.1	Hypervisor	321
B.8.1.2	M&O System	322
B.8.2	CES	323
B.8.2.1	CRS.....	323
B.8.2.2	CE	324
B.8.2.3	CO.....	324
B.8.3	Hardware-level common threat	325
Annexes C to J: Void.....		326
Annex K (normative): Generic cryptographic requirements and assessment.....		327
K.1	Cryptography.....	327
K.1.1	Requirement	327
K.1.2	Assessment of product cryptographic configuration	328
K.1.2.0	General.....	328
K.1.2.1	Assessment of ACM-listed cryptographic mechanisms.....	328
K.1.2.1.1	Assessment objective	328
K.1.2.1.2	Assessment preparation.....	328
K.1.2.1.3	Assessment activities	328
K.1.2.1.4	Assessment evidence.....	329
K.1.2.1.5	Assessment verdict.....	329
K.1.2.2	Assessment of ACM-extended cryptographic mechanisms	329
K.1.2.2.1	Assessment objective	329
K.1.2.2.2	Assessment preparation.....	329
K.1.2.2.3	Assessment activities	329
K.1.2.2.4	Assessment evidence.....	330
K.1.2.2.5	Assessment verdict.....	330
K.1.2.3	Assessment of interoperability-based cryptographic mechanisms.....	330
K.1.2.3.1	Assessment objective	330
K.1.2.3.2	Assessment preparation.....	330
K.1.2.3.3	Assessment activities	330
K.1.2.3.4	Assessment evidence.....	331
K.1.2.3.5	Assessment verdict.....	331
K.2	Crypto agility.....	331
K.2.1	Requirement	331
K.2.2	Assessment of crypto-agility	332
K.2.2.1	Assessment objective.....	332
K.2.2.2	Assessment preparation	332
K.2.2.3	Assessment activities	333
K.2.2.4	Assessment evidence	333
K.2.2.5	Assessment verdict	333
K.3	ACM-extended cryptographic mechanisms	333
K.3.1	Requirement	333
K.3.2	List of ACM-extended cryptographic mechanisms.....	334
K.3.2.1	Stream cipher mechanisms	334
K.3.2.1.1	ChaCha20.....	334
K.3.2.2	Authenticated encryption mechanisms	334
K.3.2.2.1	ChaCha20-Poly1305	334
K.3.2.3	Message authentication mechanisms	335
K.3.2.3.1	Poly1305	335
K.3.2.4	Password protection mechanisms	335
K.3.2.4.1	Argon2id	335
K.3.2.5	Elliptic-curve key agreement mechanisms	336
K.3.2.5.1	X25519 and X448	336
K.3.2.6	Digital signature mechanisms	336
K.3.2.6.1	Ed25519 and Ed448	336

K.3.2.7	Container image, artefact, attestation and metadata protection formats	337
K.3.2.7.1	COSE	337
K.3.2.7.2	JOSE / JWS / JWE	337
K.3.2.8	Protected communication profiles	338
K.3.2.8.1	QUIC	338
K.3.2.9	Secure time protocols	338
K.3.2.9.1	Network Time Security for NTP	338
K.3.2.10	Secure device and platform identity	339
K.3.2.10.1	IEEE 802.1AR secure device identity	339
K.3.3	Assessment	340
K.4	Interoperability-based cryptographic mechanisms	340
K.4.1	Requirement	340
K.4.2	List of interoperability-based cryptographic mechanisms	340
K.4.2.1	Password protection mechanisms	340
K.4.2.1.1	scrypt	340
K.4.3	Assessment	340
Annexes L to Q: Void		341
Annex R (normative):	Additional provisions for products relying on Remote Data Processing Solutions (RDPS)	342
R.1	Scope & Applicability	342
R.2	RDPS as a product-boundary extension	342
R.3	Threat Model	343
R.3.0	General	343
R.3.1	Assets	344
R.3.2	Threat catalogue	344
R.3.3	Assets ↔ Threats mapping	345
R.4	Security Requirements	345
R.4.1	General	345
R.4.2	Applicability of Annex R requirements	345
R.4.3	Local product side requirements	346
R.4.3.1	Data authenticity of interactions received from the RDPS side	346
R.4.3.2	Integrity of interactions received from the RDPS side	346
R.4.3.3	Confidentiality of data exchanged with the RDPS side	347
R.4.3.4	Availability	347
R.4.4	RDPS side requirements	348
R.4.4.1	Data authenticity of interactions received from the local product side	348
R.4.4.2	Integrity of interactions received from the local product side	349
R.4.4.3	Confidentiality of data exchanged with the local product side	349
R.4.4.4	Availability	350
R.4.5	Threats ↔ Requirements mapping	351
R.5	Conformity assessment	351
R.5.0	General	351
R.5.1	Local product side requirements	351
R.5.1.1	Assessment case for REQ-RDPS-L-AUTH-001	351
R.5.1.2	Assessment case for REQ-RDPS-L-AUTH-002	352
R.5.1.3	Assessment case for REQ-RDPS-L-AUTH-003	353
R.5.1.4	Assessment case for REQ-RDPS-L-INTEG-001	354
R.5.1.5	Assessment case for REQ-RDPS-L-INTEG-002	355
R.5.1.6	Assessment case for REQ-RDPS-L-INTEG-003	356
R.5.1.7	Assessment case for REQ-RDPS-L-CONF-001	356
R.5.1.8	Assessment case for REQ-RDPS-L-CONF-002	357
R.5.1.9	Assessment case for REQ-RDPS-L-CONF-003	358
R.5.1.10	Assessment case for REQ-RDPS-L-AVAIL-001	359
R.5.1.11	Assessment case for REQ-RDPS-L-AVAIL-002	360
R.5.1.12	Assessment case for REQ-RDPS-L-AVAIL-003	361
R.5.2	RDPS side requirements	362

R.5.2.1	Assessment case for REQ-RDPS-R-AUTH-001	362
R.5.2.2	Assessment case for REQ-RDPS-R-AUTH-002	362
R.5.2.3	Assessment case for REQ-RDPS-R-AUTH-003	363
R.5.2.4	Assessment case for REQ-RDPS-R-INTEG-001	364
R.5.2.5	Assessment case for REQ-RDPS-R-INTEG-002	365
R.5.2.6	Assessment case for REQ-RDPS-R-INTEG-003	366
R.5.2.7	Assessment case for REQ-RDPS-R-CONF-001.....	367
R.5.2.8	Assessment case for REQ-RDPS-R-CONF-002.....	368
R.5.2.9	Assessment case for REQ-RDPS-R-CONF-003.....	368
R.5.2.10	Assessment case for REQ-RDPS-R-AVAIL-001.....	369
R.5.2.11	Assessment case for REQ-RDPS-R-AVAIL-002.....	370
R.5.2.12	Assessment case for REQ-RDPS-R-AVAIL-003.....	371

Annexes S to X: Void.....	373
----------------------------------	------------

Annex Y (informative): Mapping of CES/VES cryptographic requirements to ACM and Annex K mechanism families.....	374
--	------------

Y.1 General	374
Y.2 Mapping of Hypervisor requirements	374
Y.3 Mapping of Management and Orchestration requirements	376
Y.4 Mapping of CRS requirements.....	377
Y.5 Mapping of Container Engine requirements	379
Y.6 Mapping of Container Orchestrator requirements.....	381

Annex Z (informative): Change history	382
--	------------

History	386
---------------	-----

get full document from standards.iteh.ai

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This draft Harmonised European Standard (EN) has been produced by ETSI Technical Committee Cyber Security (CYBER), and is now submitted for the combined Public Enquiry and Vote phase of the ETSI Standardisation Request deliverable Approval Procedure (SRdAP).

The present document has been prepared under the Commission's standardisation request C(2025) 618 [i.3] final to provide one voluntary means of conforming to the requirements of Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (CRA) [i.1].

Once the present document is cited in the Official Journal of the European Union under that Regulation, compliance with the normative clauses of the present document given in Table A.1 confers, within the limits of the scope of the present document, a presumption of conformity with the corresponding requirements of that Regulation and associated EFTA regulations.

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	18 months after doa

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The present document defines cybersecurity requirements applicable to Virtualisation Execution Stack (VES) and Container Execution Stack (CES), including hypervisors and container runtime systems. It applies to products with digital elements designed to host, manage, and isolate virtualised workloads and execution environments, using:

- Virtual machines (VMs): full system emulation with independent operating systems; or
- Containers: process isolation using OS-level mechanisms.

The present document supports compliance with Regulation (EU) 2024/2847, the Cyber Resilience Act, specifically addressing the essential cybersecurity requirements defined in Annex I, Parts I and II.

The present document is intended to be applied as follows:

- 1) the manufacturer identifies whether the product is a VES or a CES, and determines which components are included within the product boundary in accordance with clauses 4.1 and 4.2;
- 2) the manufacturer identifies the relevant product use case in accordance with clause 4.6 and associated risk level in accordance with clause 4.6.4 and, where needed, Annex B;
- 3) the manufacturer determines the applicable Security Profile (SP) and the corresponding requirement application logic in accordance with clause 5;
- 4) the manufacturer applies only those requirements specified in clause 5 that are relevant to the components included in the product, its intended use, and the applicable SP; and
- 5) conformity assessment is performed against the corresponding assessment provisions in clause 6.

1 Scope

The present document specifies technical requirements and corresponding assessment criteria for Virtualisation Execution Stack (VES) and Container Execution Stack (CES) products, including hypervisors and container runtime systems, related to cybersecurity. The products with digital elements in scope, thereafter referred to as the "product":

- are specified within the "technical description" of the "category of product" in Class II, point 1 by the Commission Implementing Regulation (EU) 2025/2392 [i.2] as:
"Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments";
- 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.

Commission Implementing Regulation (EU) 2025/2392 [i.2] identifies hypervisors and container runtime systems as core components. However, actual market products typically include additional elements beyond the hypervisor kernel or container runtime binary. These additional components provide essential management, orchestration, and operational capabilities that are necessary for real-world deployment and are therefore included within the scope of the present document.

The present document addresses the CRA Class II, point 1 product category within the following product contexts:

- Virtualisation Execution Stack (VES) for hypervisor-based environments; and
- Container Execution Stack (CES) for container-based environments.

The corresponding terms and definitions are provided in clause 3. The architectural decomposition, in-scope components, and security-relevant environmental dependencies are specified in clause 4.

Accordingly, the present document defines security requirements not only for the core execution systems identified in the CRA but also for the broader product context in which these systems are deployed, ensuring alignment with market reality and comprehensive coverage of security risks. The Management and Orchestration (M&O) System, Container Engine (CE), and Container Orchestrator (CO) are covered by the present document and are in scope only where they are developed or provided by the manufacturer, or under the responsibility of the manufacturer, as part of the declared product.

Any usage of AI agents is out of scope of the present document.

Where the product includes or depends on components that are outside the scope of the present document, the applicable requirements are to be addressed through the relevant operational-environment provisions or other relevant harmonised standards, as identified in clause 4.3.

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-ECCG](#): "Agreed Cryptographic Mechanisms", Version 2.0, April 2025.