



Cybersecurity (CYBER); Cyber Resilience Act (CRA); Essential cybersecurity requirements for operating systems

Exercising one of the **Principles of International Standardization – Openness** – and taking them to a different level, ETSI CYBER-EUSR has conducted open consultations on the vertical standards in support of the Cyber-Resilience Act, at a much earlier stage than it is usual in the standardization world. In this context, please keep in mind that the present document is an INTERIM draft, which expectably will be subject to substantial changes before their target publication date in the second semester of 2026.

ETSI CRA vertical standards v1.1.1 are being finalized and undergoing Public Enquiry via the National Standardization Organizations (NSO). Therefore, starting from 16 April 2026, ETSI CYBER-EUSR may only be able to address your comments in a future revision of the standard. **To enable ETSI CYBER-EUSR to address your comments before the first publication of the standards, you should cumulatively submit to your NSO any comments submitted here from 16 April 2026 onwards.** If you don't know how to do this, email us at cybersupport@etsi.org and we will guide you in the process.

Disclaimer: The INTERIM DRAFTS available for download in this page are provided for information and are for future development work within the ETSI Technical Committee CYBER EUSR Working Group (CYBER-EUSR) only. ETSI and its Members accept no liability for any further use/implementation of these specifications. Approved and published specifications and reports shall be obtained exclusively via the ETSI Documentation Service at <http://www.etsi.org/standards-search>

Commenting guidelines: Your comments to improve this early draft are very welcomed. To ensure the effectiveness of your contribution, please make sure to include the following elements in your comment:

1. Clear identification of the section of the draft your comment is referring to.
2. Objective proposal to delete content, add content or substitute content.
3. Concrete contribution (exact content you suggest including in the draft as an addition to, or in substitution of, existing content).
4. Brief rationale to justify the proposal (e.g. why the suggested content should be added an/or the existing content should be deleted or substituted).

Please note that comments without concrete contributions will be noted but not acted upon by ETSI CYBER-EUSR. We trust and value your expertise and therefore expect you to take this opportunity to proactively contribute to solving the issues you find while analysing this early draft.

Use of Artificial Intelligence (AI): Please do not use large language models to generate your comments. Inclusion of language generated by “AI” creates a potential for intellectual property conflicts and liability for ETSI, which is not acceptable.

How to comment: To comment or provide feedback on the present interim draft please visit: [STAN4CRA / EN 304 626 Operating Systems · GitLab](#) and submit your comments as “issues” following the guidelines provided on this site. Alternatively, you may also send your comments to: cybersupport@etsi.org using the “[ETSI Commenting Format for Open Consultation.xlsx](#)” available in <https://docbox.etsi.org/CYBER/EUSR/Open>

Feedback on your comments: The resolutions made in **Consensus** by ETSI CYBER-EUSR members, on each comment received through these Open Consultations will be published at the ETSI Open Area and ETSI Lab, assuring full **Transparency**.



1
2
3
4

Reference

DEN/CYBER-EUS-0016

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 may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2025.
All rights reserved.

5	1	Contents	
6		Intellectual Property Rights	7
7		Foreword.....	8
8		Modal verbs terminology	9
9		Introduction	10
10	2	Scope	11
11	2.1	General.....	11
12	2.2	Products in scope	11
13	2.2.1	General	11
14	2.2.2	Components of operating systems that are in scope.....	11
15	2.3	Products covered by other CRA harmonised standards.....	12
16	3	References	13
17	3.1	Normative references.....	13
18	3.2	Informative references	13
19	4	Definition of terms, symbols and abbreviations.....	15
20	4.1	Terms	15
21	4.2	Symbols	16
22	4.3	Abbreviations.....	17
23	5	Product context.....	18
24	5.1	Intended purpose and reasonably foreseeable use	18
25	5.2	Product functions	18
26	5.3	Product architecture	18
27	5.3.1	Overview	18
28	5.3.2	Operating system security functions	18
29	5.3.3	High-level operating system architectures	18
30	5.3.4	Access control mechanisms	19
31	5.3.5	Resource management.....	19
32	5.3.6	Scheduling.....	19
33	5.4	Operational Environment.....	20
34	5.5	Distribution of security functions	20
35	5.5.1	General	20
36	5.5.2	Security functions provided by some other part of its context	20
37	5.5.3	Security functions provided to other components	20
38	5.6	Users	20
39	5.7	Use Cases.....	20
40	5.7.1	UC-LR: Operating system for learning and research	20
41	5.7.2	UC-IoT-1: Non-internet-connected device such as a bluetooth speaker	21
42	5.7.3	UC-IoT-2: Internet-enabled power switch	21
43	5.7.4	UC-IoT-3: Internet-connected “smart home” device	21
44	5.7.5	UC-RO-1: Consumer-grade home wireless router	22
45	5.7.6	UC-OT-1: Business-grade remote door locking system.....	22
46	5.7.7	UC-MOB-1: Personal mobile device	22
47	5.7.8	UC-WE-1: Wearable health tracker	22
48	5.7.9	UC-PC-1: Personal computer in a fixed and generally safe location	23
49	5.7.10	UC-PC-2: Enterprise workstation in a fixed and generally safe location.....	23
50	5.7.11	UC-LA-1: Personal laptop	23
51	5.7.12	UC-LA-2: Enterprise laptop.....	24
52	5.7.13	UC-PS-1: Personal server.....	24
53	5.7.14	UC-SE-1: Enterprise server in a datacenter with no user accounts	24
54	5.7.15	UC-SE-2: Enterprise server in a datacenter with only trusted user accounts	25
55	5.7.16	UC-SE-3: Enterprise server in a datacenter hosting many untrusted user accounts.....	25
56	5.8	Remote data processing dependencies.....	25
57	5.8.1	General	25
58	5.8.2	RDPS-dependent product functions	25
59	5.8.3	RDPS interfaces	26

60	5.8.4	Remote data processing solutions	26
61	6	Requirements specifications.....	27
62	6.1	Notes on the structure of the Requirements	27
63	6.1.1	Necessity of Requirements.....	27
64	6.1.2	Types of Technical Requirements.....	27
65	6.1.3	Assumptions Regarding Requirements	27
66	6.2	Technical security requirements specifications	27
67	6.2.1	General.....	27
68	6.2.2	TR-NKEV: No known exploitable vulnerabilities at first use.....	28
69	6.2.3	TR-SSDD: Secure software design and development.....	28
70	6.2.4	TR-MISO: Prevent local unauthorized access of memory-addressable security-relevant data.....	30
71	6.2.5	TR-MSAF: Mitigate memory safety errors.....	31
72	6.2.6	TR-LMII: Limit incident impact.....	31
73	6.2.7	TR-MINI: Minimize impact on other devices and services	32
74	6.2.8	TR-SDEF: Secure by default configuration	33
75	6.2.9	TR-SCUD: Secure updates.....	33
76	6.2.10	TR-AUTH: Authentication and access control	34
77	6.2.11	TR-CDST: Confidentiality of data stored on the product	36
78	6.2.12	TR-CDTX: Confidentiality of data transmitted by product	36
79	6.2.13	TR-CRYP: Encryption.....	36
80	6.2.14	TR-IDST: Integrity of data stored on the product.....	37
81	6.2.15	TR-IDTX: Integrity of data transmitted by the product	37
82	6.2.16	TR-DMIN: Data Minimization	38
83	6.2.17	TR-AVAI: Availability	38
84	6.2.18	TR-LMAS: Minimize exposed interfaces.....	39
85	6.2.19	TR-LOGG: Logging and monitoring	39
86	6.2.20	TR-SCDL: Secure deletion	39
87	6.2.21	TR-SDTR: Secure data read and transfer.....	40
88	6.2.22	TR-VULH: Vulnerability handling.....	40
89	6.3	Risk Mitigation Sets.....	40
90	6.3.1	General.....	40
91	6.3.2	SP-LR required mitigations.....	41
92	6.3.3	SP-IoT-1 required mitigations.....	41
93	6.3.4	SP-IoT-2 required mitigations.....	41
94	6.3.5	SP-IoT-3 required mitigations.....	42
95	6.3.6	SP-RO-1 required mitigations.....	43
96	6.3.7	SP-OT-1 required mitigations.....	44
97	6.3.8	SP-MOB-1 required mitigations	45
98	6.3.9	SP-WE-1 required mitigations	47
99	6.3.10	SP-PC-1 required mitigations.....	48
100	6.3.11	SP-PC-2 required mitigations.....	49
101	6.3.12	SP-LA-1 required mitigations	50
102	6.3.13	SP-LA-2 required mitigations	52
103	6.3.14	SP-PS-1 required mitigations	53
104	6.3.15	SP-SE-1 required mitigations.....	54
105	6.3.16	SP-SE-2 required mitigations.....	56
106	6.3.17	SP-SE-3 required mitigations.....	57
107	7	Conformity assessment	60
108	7.1	General.....	60
109	7.2	TR-NKEV: No known exploitable vulnerabilities at first use	60
110	7.3	TR-SSDD: Secure software design and development.....	61
111	7.4	TR-MISO: Prevent local unauthorized access of memory-addressable security-relevant data	64
112	7.5	TR-MSAF: Mitigate memory safety errors	67
113	7.6	TR-LMII: Limit incident impact.....	69
114	7.7	TR-MINI: Minimize impact on other devices and services	74
115	7.8	TR-SDEF: Secure by default configuration.....	76
116	7.9	TR-SCUD: Secure updates	79
117	7.10	TR-AUTH: Authentication and access control.....	81
118	7.11	TR-CRYP: Encryption.....	86
119	7.12	TR-CDST: Confidentiality of data stored on the product.....	87

120	7.13	TR-CDTX: Confidentiality of data transmitted by product.....	89
121	7.14	TR-IDST: Integrity of data stored on the product.....	91
122	7.15	TR-IDTX: Integrity of data transmitted by the product.....	93
123	7.16	TR-DMIN: Data Minimization.....	95
124	7.17	TR-AVAI: Availability.....	95
125	7.18	TR-LMAS: Minimize exposed interfaces.....	98
126	7.19	TR-LOGG: Logging and monitoring.....	98
127	7.20	TR-SCDL: Secure deletion.....	99
128	7.21	TR-SDTR: Secure data read and transfer.....	100
129	7.22	TR-VULH: Vulnerability handling.....	101
130		Annex A (informative): Mapping between the present document and CRA requirements.....	103
131		Annex B (informative): Risk identification and assessment methodology.....	105
132		B.1 Assets.....	105
133		B.1.1 Data assets.....	105
134		B.1.2 Software assets.....	105
135		B.1.3 Hardware-interfacing assets.....	105
136		B.1.4 Network assets.....	105
137		B.1.5 Identity and access assets.....	106
138		B.1.6 Product functions.....	106
139		B.1.7 Impact of asset compromise.....	106
140		B.2 Risk factors.....	107
141		B.2.1 General comments regarding risk factors.....	107
142		B.2.2 RF-NUSR: Number of User Accounts.....	107
143		B.2.3 RF-CUSR: User Account Concurrency.....	107
144		B.2.4 RF-PPII: Potential for Collection of Personally Identifiable Information.....	107
145		B.2.5 RF-SNDS: Sensitivity of Data Stored.....	107
146		B.2.6 RF-SNDT: Sensitivity of Data Transmitted.....	107
147		B.2.7 RF-SENF: Sensitivity of Functions.....	108
148		B.2.8 RF-PHYS: Physical Access by Threat Actors to the Device.....	108
149		B.2.9 RF-UEIN: Processing of Untrusted External Inputs.....	108
150		B.2.10 RF-LOSS: Probability of Loss of the Device.....	108
151		B.2.11 RF-HWMD: Hardware Modifiability by End Users.....	108
152		B.2.12 RF-SWMD: Software Modifiability by End Users.....	108
153		B.2.13 RF-DVCS: Untrusted Peripheral Devices.....	109
154		B.2.14 RF-TNET: Access to a Public Network.....	109
155		B.2.15 RF-FNET: Accessed From Untrusted Networks Including a Public Network.....	109
156		B.2.16 RF-CONF: Configurability.....	109
157		B.2.17 RF-ADMN: Administration.....	109
158		B.2.18 RF-SUPP: Support and Foreseeable Updates.....	109
159		B.2.19 RF-RDPS: Remote data processing dependency.....	110
160		B.3 Assumptions.....	110
161		B.3.1 AS-PP: Proper platform.....	110
162		B.3.2 AS-PA: Proper administrator.....	110
163		B.3.3 AS-LP: Attacker has limited physical access to product.....	110
164		B.3.4 AS-LR: Attacker has limited resources.....	110
165		B.4 Security analysis.....	110
166		B.4.1 General.....	110
167		B.4.2 Risk assessment methodology.....	110
168		B.4.3 TH-UEVU: Unknown exploitable vulnerabilities.....	110
169		B.4.4 TH-KEVU: Known exploitable vulnerabilities.....	111
170		B.4.5 TH-UAPP: Unauthorized access to product assets via unprotected physical interfaces in default configuration.....	111
171			
172		B.4.6 TH-UAPS: Unauthorized access to product assets via unprotected local software access in default configuration.....	112
173			
174		B.4.7 TH-UAPN: Unauthorized access to product assets via unprotected network interfaces in default configuration.....	113
175			
176		B.4.8 TH-UADT: Unauthorized access to confidential data transmitted.....	113
177		B.4.9 TH-PDOS: Denial of service attack on product functions via user or network access.....	114
178		B.4.10 TH-DDOS: Denial of service attack on other products via exploitation of vulnerabilities or unauthorized use of product functions.....	114
179			

180	B.4.11 TH-MQSE: Masquerading authorized server.....	115
181	B.4.12 TH-LEAK: Data leak through side channels	115
182	B.4.13 TH-RDPS: Compromise of the remote data processing solution boundary	116
183	B.5 Mapping of use cases to risk factors	116
184	B.6 Security profiles	118
185	B.6.1 General	118
186	B.6.2 Mapping of security profiles to risk factors	118
187	Annex C (informative): Change history	120
188	7.23 History	120
189		
190		
191		

192 Intellectual Property Rights

193 **Essential patents**

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

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

203 **Trademarks**

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

208 **DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its
209 Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the
210 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of
211 the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

212

213

Foreword

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

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

222 Once the present document is cited in the Official Journal of the European Union under that Regulation, compliance
 223 with the normative clauses of the present document given in table A.1 confers, within the limits of the scope of the
 224 present document, a presumption of conformity with the corresponding requirements of that Regulation and associated
 225 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

226

227 Modal verbs terminology

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

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

232

233

Introduction

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

236 The present document supports compliance with the CRA by addressing the essential cybersecurity requirements
237 defined in Annex I, Parts I and II of the CRA, and provides a structured approach to identify the applicable
238 cybersecurity requirements for the operating systems in scope, following a risk-based approach. The security measures
239 and controls are thereby proportionate to the intended purpose, reasonably foreseeable use, deployment context, and
240 threat exposure of the product.

241 Clause 4 describes the product architecture and intended purpose in their context, and defines the Use Cases that
242 represent the main deployment scenarios reflecting the reasonably foreseeable use of the product. Use Cases serve as
243 the basis for identifying relevant cybersecurity risks.

244 Clause 5 specifies the technical cybersecurity requirements for the product. Each requirement is grouped under a
245 technical requirement (TR-XXX) and is expressed as one or more mitigations (MI-XXX). Clause 5.3 lists the Risk
246 Mitigation Sets, also known as security profiles, that determine which mitigations apply to a given product based on its
247 use case and risk factors.

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

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

251 Annex B describes the risk identification and assessment methodology used to derive the security profiles in clause 5.3.
252 Where a product does not clearly correspond to one of the Use Cases in clause 4, the methodology in Annex B may be
253 used to identify the applicable cybersecurity requirements.

254

255 2 Scope

256 2.1 General

257 The present document specifies security requirements and related assessment criteria regarding the compliance of
258 Operating Systems with EU Regulation 2024/2847 [\[i.1\]](#) Annex III, Class I, point 6.

259 The use of harmonised standards is voluntary.

260 2.2 Products in scope

261 2.2.1 General

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

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

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

274 This category includes but is not limited to:

- 275 • General purpose operating systems
 - 276 ○ Personal computing operating systems
 - 277 ○ Mobile operating systems
 - 278 ○ Server operating systems
- 279 • Special purpose operating systems
 - 280 ○ Real-time operating systems
 - 281 ○ Embedded operating systems
 - 282 ○ Single-purpose operating systems

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

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

291 2.2.2 Components of operating systems that are in scope

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

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

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

311 2.3 Products covered by other CRA harmonised standards

312 The present document does not cover product categories for which a separate CRA harmonised standard exists, even
313 where those products provide functionality that overlaps with an operating system. Examples include:

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

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

319

320 3 References

321 3.1 Normative references

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

325 Referenced documents which are not found to be publicly available in the expected location might be found in the
326 ETSI docbox.

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

329 The following referenced documents are necessary for the application of the present document.

330 [1] prEN 40000-1-1: "Cybersecurity requirements for products with digital elements - Vocabulary",
331 (produced by CEN/CENELEC).

332 NOTE: Version and date to be added upon its publication by CEN/CENELEC.

333 [2] prEN 40000-1-2: "Cybersecurity requirements for products with digital elements - Part 1-2:
334 Principles for cyber resilience", (produced by CEN/CENELEC).

335 NOTE: Version and date to be added upon its publication by CEN/CENELEC.

336 [3] prEN 40000-1-3: "Cybersecurity requirements for products with digital elements - Part 1-3:
337 Vulnerability Handling", (produced by CEN/CENELEC).

338 NOTE: Version and date to be added upon its publication by CEN/CENELEC.

339 3.2 Informative references

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

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

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

347 [i.1] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on
348 horizontal cybersecurity requirements for products with digital elements and amending
349 Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber
350 Resilience Act).

351 [i.2] Commission Implementing Regulation (EU) 2025/2392 of 28 November 2025 on the technical
352 description of the categories of important and critical products with digital elements pursuant to
353 Regulation (EU) 2024/2847 of the European Parliament and of the Council.

354 [i.3] Standardisation request M/606 - C(2025)618: "Commission Implementing decision of 3.2.2025 on
355 a standardisation request to the European Committee for Standardisation (CEN), the European
356 Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications
357 Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU)
358 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal
359 cybersecurity requirements for products with digital elements and amending Regulations (EU) No
360 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)".

361 [i.4] ETSI EN 303 645: "CYBER; Cyber Security for Consumer Internet of Things: Baseline
362 Requirements".

- 363 [i.5] EN 18031 series: "Common security requirements for radio equipment" (produced by
364 CEN/CENELEC).
- 365 [i.6] CEN/CLC JTC13: "Cybersecurity and Data Protection".
- 366 [i.7] ISO/IEC 15408: "Information security, cybersecurity and privacy protection - Evaluation criteria
367 for IT security".
- 368 [i.8] BSI CC-PP-0067: "Operating System Protection Profile".
- 369 [i.9] ISO 31000: "Risk management - Guidelines".
- 370

371 4 Definition of terms, symbols and abbreviations

372 *Editor's Note: This section needs to be updated.*

373 4.1 Terms

374 This clause provides terms and definitions based on CEN/CLC JTC13 WG09's [\[i.6\]](#) work on terms and definitions,
375 terms and definitions provided by ETSI EN 303 645 [\[i.4\]](#) and by CEN/CLC EN 18031 [\[i.5\]](#) series, and informed by
376 terms used in the Common Criteria [\[i.7\]](#) and the NIAP Operating System Protection Plan [\[i.8\]](#) guide.

377 The terms and definitions given in [1] prEN 40000-1-1 "Cybersecurity requirements for products with digital elements
378 – Vocabulary" apply and prevail where relevant. This clause introduces additional terms specific to the present
379 document.

380 For the purposes of the present document, the following terms apply.

381 **address space layout randomization (ASLR)**: anti-exploitation feature which loads memory mappings into
382 unpredictable locations

383 NOTE: ASLR makes it more difficult for an attacker to redirect control to code that they have introduced into the
384 address space of a process.

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

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

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

392 **application programming interface (API)**: specification of routines, data structures, object classes, and variables that
393 allows an application to make use of services provided by another software component, such as a library

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

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

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

398 **common criteria (CC)**: Common Criteria for Information Technology Security Evaluation (International Standard
399 ISO/IEC 15408) [\[i.7\]](#)

400 **common weakness enumeration (CWE)**: community-developed list of software and hardware weaknesses that can
401 become vulnerabilities

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

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

405 **data execution prevention**: anti-exploitation feature of modern operating systems executing on modern computer
406 hardware, which enforces a non-execute permission on pages of memory that are not code

407 NOTE: This prevents pages of memory from containing both data and instructions, which makes it more difficult
408 for an attacker to introduce and execute code.

409 **elevated privilege**: level of access that allows accessing or changing security-relevant configuration, data, or functions
410 on a system

411 **general purpose operating system**: class of operating system designed to support a wide variety of workloads
412 consisting of concurrent applications or services

413 NOTE: Typical characteristics of this category include support for third-party applications, support for multiple
 414 users, and security separation between users and their respective resources. General Purpose Operating
 415 Systems lack the operational constraints which define Special Purpose Operating Systems, including Real
 416 Time Operating System (RTOS), that are typically used in routers, switches, and embedded devices.

417 **input/output (I/O)**: process or function for passing data to or from a given process over a specific interface

418 NOTE: Such I/O interfaces include, but are not limited to, serial ports, network ports, long-term storage devices
 419 including hard drives and flash drives, as well as human-interface ports such as display and audio devices.

420 **memory protection unit (MPU)**: hardware component that enforces access permissions on memory regions without
 421 address translation, commonly used on platforms without a memory management unit (MMU)

422 **memory-safe language**: programming language whose type system or runtime prevents, by default, out-of-bounds
 423 memory access, use-after-free, double-free, and buffer overflow

424 **non-writable executable memory**: anti-exploitation feature of modern operating systems executing on modern
 425 computer hardware, which enforces a non-write permission on pages of memory that are code

426 NOTE: This prevents modifying the instructions of running programs, which makes it more difficult for an
 427 attacker to introduce and execute code.

428 **operating system (OS)**: software products with digital elements that provide an abstract interface of the underlying
 429 hardware and control the execution of software, and that may provide services such as computing resource management
 430 and configuration, scheduling, input-output control, managing data, and providing an interface through which
 431 applications interact with system resources and peripherals. This category includes but is not limited to real-time
 432 operating systems, general-purpose and special-purpose operating systems

433 **personally identifiable information (PII)**: any information about an individual maintained by an agency, including but
 434 not limited to, education, financial transactions, medical history, and criminal or employment history and information
 435 which can be used to distinguish or trace an individual's identity

436 **principle of least privilege**: design principle requiring that users, processes, and interfaces are granted only the
 437 minimum level of permission necessary to perform their legitimate functions, and nothing more

438 **process isolation**: techniques to prevent processes from accessing or changing each other's state

439 **remote data processing solution (RDPS)**: data processing at a distance for which the software is designed and
 440 developed by the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent
 441 the product from performing one of its functions

442 NOTE: SOURCE: Regulation (EU) 2024/2847, Article 3, point 2 [\[i.1\]](#).

443 **residual risk**: risk remaining after risk treatment has been applied [\[i.9\]](#)

444 **sensitive data**: sensitive data may include all user or enterprise data or may be specific application data such as PII,
 445 emails, messaging, documents, calendar items, contacts, credentials, and keys

446 **system call interface**: specification for the API between the application layer and the kernel or system layer

447 **threat actor**: entity that can adversely affect the system through malicious or unauthorized activities

448 **unsafe memory features**: features of a memory-safe language that bypass its default memory safety guarantees,
 449 typically accessed through explicit compiler directives or library functions

450 **user**: entity that is subject to configuration policies applied to the operating system by administrators

451 NOTE: On some systems under certain configurations, a normal user can temporarily elevate privileges to that of
 452 an administrator. At that time, such a user should be considered an administrator.

453 **user account**: identity created in an operating system with associated access controls and privileges

454 NOTE: Users may have multiple user accounts and user accounts may have multiple users.

455 4.2 Symbols

456 Void.

457

4.3 Abbreviations

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

API	Application Programming Interface
ASLR	Address Space Layout Randomization
BMC	Baseboard Management Controller
CC	Common Criteria
CPU	Central Processing Unit
CRA	Cyber Resilience Act
CWE	Common Weakness Enumeration
I/O	Input/Output
MMU	Memory Management Unit
MPU	Memory Protection Unit
OS	Operating System
PII	Personally Identifiable Information
RDPS	Remote Data Processing Solution
RF	Risk Factor
RTOS	Real-Time Operating System
SA	Security Assurance Level
SP	Security Profile
UC	Use Case

459

460 5 Product context

461 5.1 Intended purpose and reasonably foreseeable use

462 The intended purpose of this product is to provide an abstract interface of the underlying hardware and control the
463 execution of software, and potentially provide services such as computing resource management and configuration,
464 scheduling, input-output control, managing data, and providing an interface through which applications interact with
465 system resources and peripherals.

466 Its reasonably foreseeable use is to facilitate the use of computing hardware and serve as a platform for other software.

467 5.2 Product functions

468 The functions of an operating system commonly include process isolation, memory isolation, I/O abstraction, device
469 driver management, user authentication and access control, event logging, software management, device firmware
470 management, and secure updates.

471 5.3 Product architecture

472 5.3.1 Overview

473 An operating system abstracts the hardware, allocates resources, and provides services to itself and any other software
474 on the system. It often serves as a central organizing authority that controls access to system resources by various pieces
475 of software, dividing up available resources among the applications and its own subsystems to meet implicit or explicit
476 goals or constraints. An operating system often uses a large part of the resources of the system it runs on, but in return it
477 simplifies the development and deployment of the overall system.

478 Operating system architecture varies widely and depends on many factors, including the intended use case, the
479 underlying platform, and the design philosophy of the developers. This overview will focus on the elements of
480 operating system architecture that have a significant impact on the security functions and risk mitigations of an
481 operating system.

482 5.3.2 Operating system security functions

483 The security of an operating system relies heavily on properly controlling the instructions executed by the system
484 processor. Instruction flow is dependent on the program instructions, any data it accesses, and any hardware that has the
485 ability to change either data or which instructions are being executed.

486 Example #1: a network interface adapter can write directly to system memory, potentially altering data values and
487 thereby influencing the behavior of running programs or even causing unintended code execution.

488 Example #2: a USB controller can raise an interrupt which can cause the interrupt controller to force the CPU to switch
489 to executing interrupt handling code, altering the instruction flow.

490 A fundamental building block of most operating systems is the principle of “privilege”. Privilege determine which
491 system resources or functions a program is allowed to access. The operating system grants a specific set of privileges to
492 itself, its subsystems, and user-level programs, ensuring that each component operates within defined boundaries to
493 maintain system security and stability.

494 Generally, privileges are enforced using hardware features such as a memory management unit and processor-defined
495 privilege levels. If the hardware does not provide these features, the operating system may use a best effort approach,
496 such as relying on the compiler to generate code that is less likely to accidentally interfere with the functions of the
497 operating system or other parts of the system.

498 5.3.3 High-level operating system architectures

499 Operating systems architecture can vary in many ways which significantly affect security outcomes for the product. For
500 this reason, the present document does not attempt to define specifics of operating system architecture. Some examples
501 of differences include:

- 502 • the proportion of operating system code executed with different privileges;
- 503 • whether application code is executed with the same privileges as the operating system;

- 504 • the method of communication between processes with different privileges;
- 505 • the degree of reliance on hardware capabilities to enforce privilege separation and process isolation.

506 Each of these design variations makes different tradeoffs between security, performance, and ease of implementation.

507 A few common operating system architectures are described below for reference, but should not be taken normatively.

508 **Monolithic kernel:** The operating system kernel is one executable running at the highest processor privilege level in
 509 one memory domain, providing the majority of system-wide services. Applications are in separate memory domains and
 510 have a lesser privilege level. Applications request services and resources via system calls. Often a monolithic kernel
 511 supports modules, which allows parts of the kernel to be added or removed at run-time, but they are usually sharing the
 512 same memory domain and privilege level.

513 **Microkernel:** The operating system kernel running at the highest processor privilege level provides a minimal set of
 514 resource allocation services, while many of the operating system services are provided by separate executables with
 515 lower privileges.

516 **Hybrid kernel:** A mix of microkernel and monolithic kernel, where some operating system services are provided in the
 517 central kernel and some are provided by applications. Subsystems that do not need to be high performance and are a
 518 frequent source of vulnerabilities are often moved into applications, such as printer drivers or file systems with complex
 519 features or low performance requirements.

520 **Exokernel:** The operating system does not abstract the resources of the system, it only manages resource allocation
 521 between different applications.

522 **Unikernel:** The operating system and the application are effectively a single executable. Often this is described as a
 523 library operating system: a set of library routines that an application can include and effectively become the operating
 524 system.

525 5.3.4 Access control mechanisms

526 Operating systems may control access to resources in different ways, including but not limited to:

- 527 • Access control lists: Each resource has a list of users or processes that are allowed to access it.
- 528 • Role-based access control: Users are assigned one or more roles, and roles have permissions associated with
 529 them.
- 530 • Capabilities: Access to a resource is linked to a token which can be passed between processes.

531 5.3.5 Resource management

532 Operating systems may control resource management in different ways, including but not limited to imposing per-
 533 process limitations on processor time, memory allocation, storage usage, number of file descriptors, or number of
 534 process table entries.

535 Operating systems may implement limits on the number or proportion of specific resources that an application or thread
 536 may use, and may group these limits by user, process, process group, or other mechanism.

537 5.3.6 Scheduling

538 Operating systems may provide voluntary or involuntary switching between different processes, and may rely on
 539 hardware capabilities to improve or limit parallel process execution and isolation.

540 Some common models include:

541 **Cooperative scheduling:** Each thread runs until it voluntarily yields control of the processor to another thread. No
 542 thread is interrupted unless it explicitly yields the CPU.

543 **Preemptive scheduling:** Threads can be involuntarily suspended by the scheduler and replaced with other threads, and
 544 they may also voluntarily yield the CPU.

545 Operating systems may perform scheduling based on many factors, such as but not limited to:

- 546 • Time spent executing during a previous time period
- 547 • Time since the thread was first marked runnable

- 548 • Explicit priorities associated with each thread
- 549 • Type of thread (kernel or application)
- 550 • Resource limits
- 551 • Performance considerations

552 5.4 Operational Environment

553 The operational environment of an operating system is highly varied. In general it includes at least a platform (virtual or
 554 physical), and may also include applications, separately shipped device drivers, device firmware, peripherals, and many
 555 other components. Operating systems may be a standalone software product on a single processor, or it may be part of
 556 suite of software products running on multiple processors. Many systems have multiple operating systems all managing
 557 different parts of the system at the same time.

558 5.5 Distribution of security functions

559 5.5.1 General

560 For each security requirement, a product may:

- 561 • Provide the necessary security function(s) itself
- 562 • Require security functions be provided by some other part of its context
- 563 • Provide security functions for the use of other components

564 Most individual hardware components do not have a built-in method of secure firmware update, and rely on the
 565 presence of an operating system which can update the component's firmware securely.

566 5.5.2 Security functions provided by some other part of its context

567 Operating systems often rely on essential external functionality to implement their necessary security functionality.

568 For example, many operating systems rely on hardware secure elements and a compatible boot manager prior to the
 569 beginning of the operating system's own execution in order for the operating system to execute securely.

570 5.5.3 Security functions provided to other components

571 Operating systems often provides essential security functions to other components of the system.

572 5.6 Users

573 Users of products may interact directly with the operating system, or the operating system may be integrated into a
 574 product in such a way that the end user does not interact directly with any functionality of the operating system.

575 5.7 Use Cases

576 *Editor's Note: The following list of use cases is an illustrative set of possible use cases selected to demonstrate the*
 577 *mechanics of this standard and provide clear guidance for the most common product categories.*

578 *Editor's Note: Considering that Operating Systems provide an essential functionality for all Digital Products, it is not*
 579 *feasible to list in detail either all extant or all potential use cases for operating systems.*

580 *Editor's Note: We anticipate that future revisions of this document may include additional use cases, such as for the*
 581 *following product scenarios: embedded devices, baseband management controllers, network interface cards, graphics*
 582 *cards, real-time applications, and special purpose operating systems.*

583 5.7.1 UC-LR: Operating system for learning and research

584 **Product characteristics:**

- 585 • does not store any sensitive or useful data

586 **Operational environment:**

- 587
- security is provided entirely by the environment

588 **User expectations:**

- 589
- used only for learning and research
- 590
- the user is expected to modify the product extensively

591 **5.7.2 UC-IoT-1: Non-internet-connected device such as a bluetooth**
592 **speaker**593 **Product characteristics:**

- 594
- does not store any user-specific data
- 595
- has no means to connect directly to a public network

596 **Operational environment:**

- 597
- no specific environmental requirements

598 **User expectations:**

- 599
- not intended to support hardware, software, or operating system changes

600 **5.7.3 UC-IoT-2: Internet-enabled power switch**601 **Product characteristics:**

- 602
- stores account information to authenticate to WiFi and to cloud service provider
- 603
- has a minimalistic interface, such as a single button for pairing and a reset button
- 604
- connects to a manufacturer-operated central service for remote data processing

605 **Operational environment:**

- 606
- does not have accessible I/O ports

607 **User expectations:**

- 608
- not intended for end-user hardware, software, or operating system modification

609 **5.7.4 UC-IoT-3: Internet-connected “smart home” device**

610 e.g. a thermostat, fridge, or alarm system

611 **Product characteristics:**

- 612
- stores account information to authenticate to WiFi and to cloud service provider
- 613
- may display personalized information, such as location-specific weather forecast
- 614
- connects to a manufacturer-operated central service for remote data processing

615 **Operational environment:**

- 616
- does not have accessible I/O ports

617 **User expectations:**

- 618
- does not support arbitrary file storage or end-user operating system configuration changes
- 619
- serviced by trained professionals who do not modify software or hardware outside of manufacturer
- 620
- specifications

621 5.7.5 UC-RO-1: Consumer-grade home wireless router

622 **Product characteristics:**

- 623 • stores account information for authentication with ISP

624 **Operational environment:**

- 625 • is exposed to the open internet

626 **User expectations:**

- 627 • not intended for end-user hardware or software modification

628 5.7.6 UC-OT-1: Business-grade remote door locking system

629 **Product characteristics:**

- 630 • does not store any user data
- 631 • hardware likely contains tamper-evident signals which the operating system can rely on

632 **Operational environment:**

- 633 • is not exposed to the open internet and is only connected to trusted networks
- 634 • does not have accessible I/O ports

635 **User expectations:**

- 636 • not intended for hardware or software modification
- 637 • only serviced by professionals

638 5.7.7 UC-MOB-1: Personal mobile device

639 **Product characteristics:**

- 640 • stores highly sensitive personal information
- 641 • large number of sensors allow mass collection of sensitive personal data
- 642 • device is often always on and always connected

643 **Operational environment:**

- 644 • device usage is not limited to trusted locations and loss is foreseeable
- 645 • size and cost make it a common target of theft
- 646 • device frequently connects to untrusted networks

647 **User expectations:**

- 648 • hardware and operating system configuration not intended for modification by users
- 649 • end-users frequently install software of uncertain provenance
- 650 • device frequently collects user's location at all times

651 5.7.8 UC-WE-1: Wearable health tracker

652 e.g. a smart watch or step tracker

653 **Product characteristics:**

- 654 • stores information about a single user only

- 655 • stored information may be highly sensitive and is likely to be strictly structured (not arbitrary files)
- 656 • connects to a manufacturer-operated central service for remote data processing

657 **Operational environment:**

- 658 • does not have accessible I/O ports
- 659 • connections are proxied by a trusted device, such as a mobile phone
- 660 • is not exposed to a public network

661 **User expectations:**

- 662 • not user-modifiable

663 5.7.9 UC-PC-1: Personal computer in a fixed and generally safe location

664 **Product characteristics:**

- 665 • stores personal information and arbitrary files

666 **Operational environment:**

- 667 • foreseeably connects to a public network and to low-trust local networks, but is not reachable from the open
- 668 internet

669 **User expectations:**

- 670 • hardware, software and operating system may be configured and modified by the end-user
- 671 • the user may not be highly skilled or an authorized representative of the manufacturer

672 5.7.10 UC-PC-2: Enterprise workstation in a fixed and generally safe 673 location

674 **Product characteristics:**

- 675 • stores business data, personal information and arbitrary files
- 676 • hardware likely contains tamper-evident indicators and secure elements for cryptographic storage

677 **Operational environment:**

- 678 • installed in an access-controlled workspace
- 679 • connected to a public network with external mitigations, such as enterprise-grade firewalls
- 680 • connects to trusted local networks

681 **User expectations:**

- 682 • serviced by trained professionals who may modify both software and hardware
- 683 • used for web browsing

684 5.7.11 UC-LA-1: Personal laptop

685 **Product characteristics:**

- 686 • stores personal information and arbitrary files
- 687 • hardware likely contains tamper-evident indicators and secure elements for cryptographic storage

688 **Operational environment:**

- 689 • device is a foreseeable target of theft and tampering by untrusted 3rd parties

- 690 • unrestricted connection to a public network
- 691 • is frequently connected to untrusted networks

692 **User expectations:**

- 693 • hardware, software and operating system may be configured and modified by the end-user

694 5.7.12 UC-LA-2: Enterprise laptop

695 **Product characteristics:**

- 696 • stores business data, personal information and arbitrary files
- 697 • hardware likely contains tamper-evident indicators and secure elements for cryptographic storage

698 **Operational environment:**

- 699 • device is a foreseeable target of theft and tampering by untrusted 3rd parties
- 700 • unrestricted connection to a public network
- 701 • is frequently connected to untrusted networks

702 **User expectations:**

- 703 • serviced by trained professionals (administrators) who can modify both software and hardware
- 704 • hardware, software and operating system can be configured and modified by the end-user within restrictions
- 705 set by administrators

706 5.7.13 UC-PS-1: Personal server

707 **Product characteristics:**

- 708 • always stationary, access to hardware interfaces unlikely

709 **Operational environment:**

- 710 • installed in a fixed location at home or in a cohosting facility
- 711 • connected to a public network with a firewall
- 712 • connects to trusted local network
- 713 • limited access permitted from a public network for specific services

714 **User expectations:**

- 715 • one or a small number of trusted users
- 716 • semi-professional semi-automated management by one or a few people

717 5.7.14 UC-SE-1: Enterprise server in a datacenter with no user accounts

718 **Product characteristics:**

- 719 • hardware likely contains tamper-evident indicators and secure elements for cryptographic storage

720 **Operational environment:**

- 721 • installed in a monitored and secured facility
- 722 • connected to a public network with external mitigations, such as enterprise-grade firewalls
- 723 • connects to trusted local networks

724 **User expectations:**

- 725 • serviced by trained professionals who may modify both software and hardware

726 5.7.15 UC-SE-2: Enterprise server in a datacenter with only trusted user 727 accounts

728 **Product characteristics:**

- 729 • hardware likely contains tamper-evident indicators and secure elements for cryptographic storage

730 **Operational environment:**

- 731 • installed in a monitored and secured facility
- 732 • connected to a public network with external mitigations, such as enterprise-grade firewalls
- 733 • connects to trusted local networks

734 **User expectations:**

- 735 • serviced by trained professionals who may modify both software and hardware
- 736 • user accounts are restricted to trusted users

737 5.7.16 UC-SE-3: Enterprise server in a datacenter hosting many untrusted 738 user accounts

739 **Product characteristics:**

- 740 • hardware likely contains tamper-evident indicators and secure elements for cryptographic storage

741 **Operational environment:**

- 742 • installed in a monitored and secured facility
- 743 • connected to a public network with external mitigations, such as enterprise-grade firewalls
- 744 • connects to trusted local networks

745 **User expectations:**

- 746 • serviced by trained professionals who may modify both software and hardware
- 747 • user accounts include untrusted users

748 5.8 Remote data processing dependencies

749 5.8.1 General

750 This clause identifies product functions that depend on remote data processing solutions within the scope of the present
751 document, the interfaces through which the product communicates with those remote data processing solutions, and the
752 remote data processing solutions themselves. Where the product depends on a remote data processing solution for the
753 operation of a product function, the risk factor RF-RDPS-01 applies. The requirements that mitigate risks introduced at
754 the product-to-remote-data-processing-solution boundary are listed in clause 5 and are gated by the applicability
755 condition “Product depends on one or more remote data processing solutions”.

756 The scope of the present document with respect to remote data processing solutions is limited to the boundary between
757 the product and the remote data processing solution, namely the product-side endpoint and the interactions exchanged
758 across that boundary. The present document does not extend the scope of the product to the remote service environment
759 or underlying third-party infrastructure.

760 5.8.2 RDPS-dependent product functions

761 The following product functions are RDPS-dependent within the scope of the present document:

- 762 • Cloud-backed authentication and account management for use cases where the product authenticates the end
763 user against a manufacturer-operated service (UC-IoT-2, UC-IoT-3, UC-WE-1).
- 764 • Telemetry, attestation, and health reporting from the product to a manufacturer-operated service (UC-IoT-2,
765 UC-IoT-3, UC-WE-1).
- 766 • Update orchestration and device-management interactions where the product receives configuration, security-
767 relevant commands, or update metadata from a manufacturer-operated service (UC-IoT-2, UC-IoT-3, UC-WE-
768 1).

769 5.8.3 RDPS interfaces

770 The interface between the product and a remote data processing solution is the communication boundary between the
771 product-side endpoint (client, agent, or connector running on the product) and the remote-data-processing-solution-side
772 endpoint (service endpoint exposed by the remote data processing solution). This interface typically traverses a public
773 network and is not under the control of the user of the product. Communication across this interface is assumed to be
774 conducted over a secure channel and to be authenticated at the endpoint level.

775 5.8.4 Remote data processing solutions

776 A remote data processing solution within the scope of the present document is a manufacturer-operated service, or a
777 service operated under the responsibility of the manufacturer, the absence of which would prevent the product from
778 performing one or more of its functions. For the use cases identified in clause [4.8.2](#), the remote data processing solution
779 is typically a manufacturer-operated cloud service providing authentication, update distribution, or device-management
780 endpoints.

781 The present document assumes that the remote data processing solution is subject to security controls applied by its
782 operator and that the trust relationship between the product and the remote data processing solution is established at
783 product initialization time through credentials or trust anchors provisioned by the manufacturer or the integrator.

784

785 6 Requirements specifications

786 6.1 Notes on the structure of the Requirements

787 *Editor's Note: The CRA requires the manufacturer to keep all the documentation necessary to show that the tests were*
788 *conducted. In Article 13 Rec. 22, MSA's are granted the right to request "all the information and documentation, in*
789 *paper or electronic form, necessary to demonstrate the conformity of the product with digital elements and of the*
790 *processes put in place by the manufacturer with the essential cybersecurity requirements set out in Annex I." The*
791 *objective of these requirements is to provide manufacturers with sufficient guidance to consistently satisfy such requests*
792 *from the market authorities.*

793 6.1.1 Necessity of Requirements

794 Not all requirements are necessary for all products. The mapping table at the end of each requirement enumerates the
795 set of risk factors and product use cases for which the requirements are necessary. See Annex B for more information.

796 6.1.2 Types of Technical Requirements

797 All technical requirements in the present document specify properties of the product or obligations of the manufacturer
798 that are verifiable. Verification is performed through assessment activities defined alongside each mitigation in clause
799 5.2.

800 Where a product property can be verified by testing the product directly, the assessment activity is a test procedure with
801 a measurable verdict.

802 Where a product property cannot be verified by testing the product directly, the assessment activity is a documentation
803 review. In this case the manufacturer shall provide supporting documentation as conformity assessment evidence. The
804 documentation does not replace the product property. It demonstrates that the property holds.

805 NOTE: Simple process statements (e.g., a statement that something has been done, without supporting evidence)
806 are not acceptable as conformity assessment evidence.

807 6.1.3 Assumptions Regarding Requirements

808 6.1.3.1 Testability

809 Manufacturers are already required to provide the ability to enable testing and collect output on the product as placed on
810 the market, and will supply instructions for enabling and collecting test data.

811 6.1.3.2 Source Code

812 The market authorities may request source code access as part of a verification process, if necessary.

813 6.1.3.3 Mitigations

814 Mitigations are the technical means by which a technical requirement is satisfied. Each mitigation's applicability to a
815 given product is determined by the risk factors and security profile mappings in clause 5.3 and Annex B.

816 NOT ALL MITIGATIONS ARE NECESSARY FOR ALL USE CASES. See Section 5.3 for the mappings of security
817 profiles to mitigations and Annex B for additional information.

818 6.1.3.4 Residual risk

819 Some cybersecurity risks cannot be fully eliminated by the product alone and result in residual risk after the product's
820 mitigations have been applied. Where this is the case, the manufacturer shall document the residual risk and the actions
821 the user or the operational environment can take to address it.

822 6.2 Technical security requirements specifications

823 6.2.1 General

824 This clause specifies the technical cybersecurity requirements for operating systems. Each technical requirement (TR-
825 XXX) is satisfied by implementing the mitigations (MI-XXX) listed under it. The set of mitigations that a given product

826 shall implement is determined by the security profile assigned to that product in clause 5.3. A mitigation that also
 827 carries an applicability field applies only when the stated condition holds for the product. Compliance with a technical
 828 requirement is demonstrated by passing the assessment activities defined for each applicable mitigation.

829 6.2.2 TR-NKEV: No known exploitable vulnerabilities at first use

830 6.2.2.1 General

831 This clause addresses CRA Annex I, Part 1, (2)(a): products shall be placed on the market without known exploitable
 832 vulnerabilities. It groups mitigations that verify the product is free of known exploitable vulnerabilities at market
 833 placement through documentation review, manual testing, automated scanning, or a combination of these.

834 For operating systems, identification of known exploitable vulnerabilities spans the kernel, system libraries, device
 835 drivers, pre-installed applications, and any package management system provided by the product. The manufacturer
 836 shall consider upstream security advisories from component maintainers in addition to the manufacturer's own
 837 vulnerability research. Automated scanners selected for operating systems should cover kernel vulnerabilities, system
 838 library vulnerabilities, and installed application vulnerabilities. Privilege escalation vulnerabilities warrant particular
 839 attention as they are characteristic of operating system attack surfaces.

840 6.2.2.2 MI-KEVM: Documentation of mitigation of known exploitable vulnerabilities

841 The product shall be accompanied by documentation demonstrating that all known exploitable vulnerabilities have been
 842 identified and either remediated or documented with the residual risk and any compensating control. The product is
 843 deemed to be compliant with this requirement if it:

844 - has no known exploitable vulnerabilities

845 - has known exploitable vulnerabilities that were disclosed within the manufacturer's documented vulnerability
 846 remediation timeline and for which remediation is in progress

847 - for each remaining vulnerability, has documentation of the residual risk and any compensating control

848 6.2.2.3 MI-KEVT: Testing for known exploitable vulnerabilities

849 Before release, the product shall undergo verification that all known exploitable vulnerabilities have been mitigated.
 850 Verification may use manual testing, automated scanning, or both. The product is deemed to be compliant with this
 851 requirement if it:

852 - has no known exploitable vulnerabilities

853 - has known exploitable vulnerabilities that were disclosed within the manufacturer's documented vulnerability
 854 remediation timeline and for which remediation is in progress

855 - for each tested vulnerability, the test result shows that the vulnerability has been mitigated

856 6.2.2.4 MI-SCAN: No scannable known exploitable vulnerabilities

857 The results of automated vulnerability scanners shall be used as inputs to the manufacturer's vulnerability handling
 858 process. Reported issues shall be triaged according to the manufacturer's documented secure development and
 859 vulnerability remediation policy, including severity classification, exploitability assessment, and compensating controls.
 860 The manufacturer shall document the disposition of scanner-reported issues in accordance with its vulnerability
 861 handling process.

862 • Applicability: Automated vulnerability scanners are available for the product

863 6.2.3 TR-SSDD: Secure software design and development

864 6.2.3.1 General

865 This clause addresses CRA Annex I, Part 1, (1): cybersecurity by design. It groups mitigations that verify the absence of
 866 exploitable weaknesses in the product as delivered. The mitigations cover verification of memory safety through source
 867 code analysis, runtime testing, boundary testing, memory-safe language adoption, and formal verification.

868 **6.2.3.2 MI-SSCA: Static source code analysis for memory errors in memory unsafe**
 869 **languages**

870 All security-relevant parts of the product shall be checked for memory errors using a source code analysis tool that
 871 detects code that may produce common memory errors, such as:

- 872 - buffer overflow
- 873 - out-of-bounds
- 874 - use after free
- 875 - double free
- 876 - use of uninitialized variables
- 877 - dereference of invalid pointer

878 The manufacturer shall document the criteria used to select the source code analysis tool and to configure its runtime,
 879 and shall justify that those criteria cover the memory error classes listed above. All warnings, annotations, or other
 880 methods of suppressing warnings from the analysis tool shall be documented with the residual risk and any
 881 compensating control. Where a class of warnings is known to have a high false positive rate, the manufacturer may
 882 document the class-level rationale once rather than per warning.

883 **6.2.3.3 MI-FZ95: Runtime code coverage checking with memory access error detection**

884 The product shall be checked for memory errors by running a tool that exercises the functions of the product in an
 885 environment that permits measuring code coverage and detecting memory access errors. Each detected memory error
 886 shall be either remediated, or documented with the residual risk and any compensating control.

887 **6.2.3.4 MI-IMSL: Implement in a memory-safe language**

888 The product's firmware and/or software shall be implemented in a memory-safe language. Any use of unsafe memory
 889 features shall be documented to explain why they are necessary and do not present a security risk.

890 **6.2.3.5 MI-BTIN: Boundary testing of inputs that may cause memory errors**

891 The input fields of the product that may produce memory errors in the firmware or device driver shall be identified. The
 892 product shall be boundary tested for all such inputs while monitoring for memory errors. Each detected memory error
 893 shall be either remediated, or documented with the residual risk and any compensating control.

894 **6.2.3.6 MI-SCFS: Secure compilation flags**

895 The product binary shall exhibit the hardening measures documented by the manufacturer for the target platform and
 896 language. The manufacturer shall document the set of compilation flags and options used, including the rationale for
 897 each flag and any exceptions or limitations. Each exception shall be documented with the residual risk and any
 898 compensating control.

- 899 • Applicability: Product implemented in a compiled language

900 **6.2.3.7 MI-FVFC: Formal verification of functional correctness**

901 All security-relevant parts of the product shall be formally proved correct with respect to a formal specification using a
 902 sound formal verification tool that produces a formal proof of conformity between the source code and the formal
 903 specification. Such a proof may imply the absence of common memory errors, such as:

- 904 - buffer overflow
- 905 - out-of-bounds
- 906 - use after free
- 907 - double free
- 908 - use of uninitialized variables
- 909 - dereference of invalid pointer

910 The sufficiency of the formal verification tool and the formal specification shall be documented. The process to run the
 911 formal verification tool to produce a formal proof shall be documented. An explicit list of the assumptions required for
 912 the mitigation to apply to the running product shall be documented, in enough detail to know what should be checked in
 913 practice on the product to ensure that the assumptions are indeed being met.

914 6.2.4 TR-MISO: Prevent local unauthorized access of memory- 915 addressable security-relevant data

916 6.2.4.1 General

917 This clause groups mitigations that prevent unauthorized access to memory-addressable security-relevant data by code
 918 running on the product. It covers hardware-enforced memory access control, isolation between user accounts, and the
 919 prevention or documentation of microarchitectural side-channel data leaks. Memory-addressable data includes system
 920 memory, storage addressable via memory mapping, memory for I/O devices, and anything else accessible via the
 921 memory-related instructions in the platform. The clause does not cover unauthorized access by elements of the platform
 922 the product runs on, such as CPU microcode, devices on the system bus, other operating systems in the device, or a
 923 hypervisor.

924 6.2.4.2 MI-MMAC: Memory access control

925 The product shall implement mandatory hardware-enforced access control to memory, or an equivalent software-
 926 enforced isolation mechanism documented by the manufacturer, to prevent unauthorized access of memory.

- 927 • Applicability: Has user accounts

928 6.2.4.3 MI-CCON: Prevent creation of more than one user account

929 The product shall prevent the creation of a user account if one already exists.

- 930 • Applicability: Has user accounts

931 6.2.4.4 MI-UCON: Prevent concurrent user account usage

932 The product shall prevent a user account from logging in if another user account is already logged in.

- 933 • Applicability: Has user accounts

934 6.2.4.5 MI-PMSC: Prevent memory leaks through microarchitectural side channels in 935 provided executables

936 The product shall implement mechanisms to prevent the executables it provides from leaking memory data to
 937 unauthorized users through known exploitable microarchitectural side channels (MASCs), such as via the observing the
 938 time of cache access for various operations including:

- 939 - speculative execution/loads/stores
- 940 - branch prediction
- 941 - out-of-order execution
- 942 - shared multithreading resources
- 943 - address translation
- 944 - memory access patterns
- 945 - prefetching

946 6.2.4.6 MI-RRMD: Document residual risk of microarchitectural side channel data leaks

947 The documentation provided to the user shall describe the risk of microarchitectural side channel data leaks and shall
 948 provide the configuration steps and operational practices documented by the manufacturer for mitigating that risk.

- 949 • Applicability: (for requirements that depend on a feature)

950 6.2.5 TR-MSAF: Mitigate memory safety errors

951 6.2.5.1 General

952 Memory safety errors are a recurring source of exploitable vulnerabilities in operating systems written in memory-
 953 unsafe languages. This clause groups mitigations that prevent the product from reading or writing memory outside the
 954 bounds of validly allocated regions, and that detect use-after-free and double-free conditions. Requirements and
 955 assessment procedures are stated in terms of execution contexts. On products with kernel/userspace privilege
 956 separation, kernel and userspace are the execution contexts to assess. On products without privilege separation, all
 957 requirements apply to the single execution context.

958 6.2.5.2 MI-MSAF-1: Stack exhaustion detection

959 The product shall reject writes beyond the end of the stack in every execution context.

960 6.2.5.3 MI-MSAF-2: Stack linear buffer overflow detection

961 The product shall reject stack buffer writes that go beyond the end of the stack frame in every execution context.

962 6.2.5.4 MI-MSAF-3: Array bounds checking

963 The product shall reject writes to fixed-size arrays that are outside the bounds of the array in every execution context.

964 6.2.5.5 MI-MSAF-4: Heap linear buffer overflow detection

965 The product shall reject writes beyond the bounds of allocated heap memory in every execution context.

- 966 • Applicability: Product uses dynamic memory allocation

967 6.2.5.6 MI-MSAF-5: Heap use-after-free access prevention

968 The product shall reject use of allocated memory that has been freed in every execution context.

- 969 • Applicability: Product uses dynamic memory allocation

970 6.2.5.7 MI-MSAF-6: Heap free checking

971 The product shall reject freeing of memory that was allocated and previously freed in every execution context.

- 972 • Applicability: Product uses dynamic memory allocation

973 6.2.6 TR-LMII: Limit incident impact

974 6.2.6.1 General

975 This clause groups defence-in-depth controls that constrain the impact of memory bugs at the operating system layer.
 976 The mitigations cover both systems with kernel/userspace privilege separation and systems that use alternative isolation
 977 mechanisms such as a memory protection unit (MPU). Where a mitigation requires a specific architectural feature, the
 978 applicability field states the condition.

979 6.2.6.2 MI-MZRO-1: Stack memory zeroing

980 Both kernel and userspace threads shall zero-initialize all stack memory before use.

981 6.2.6.3 MI-MZRO-2: Heap memory zeroing

982 Both kernel and userspace threads shall zero-initialize all heap memory before use.

983 6.2.6.4 MI-MRWX-1: Prevent writes to executable and read-only data memory

984 Both kernel and userspace threads shall reject writes to executable and read-only data memory mappings

985 6.2.6.5 MI-MRWX-2: Prevent execution of non-kernel code memory

986 Kernel threads shall prevent execution of non-kernel code memory.

987 **6.2.6.6 MI-ASLR: Address space layout randomization**

988 The product shall enable Address Space Layout Randomization (ASLR) by default for all executables, including the
989 kernel, if any.

- 990 • Applicability: Platform has an MMU and product implements virtual memory

991 **6.2.6.7 MI-MRCO: Mitigate reference counter overflow**

992 Both kernel and userspace threads shall mitigate the effects of reference counter overflows

993 **6.2.6.8 MI-NKAM: Prevent unintentional kernel access to userspace memory**

994 Kernel threads shall prevent cross-privilege memory access.

- 995 • Applicability: Product has multiple privilege levels

996 **6.2.6.9 MI-PULS: Prevent use of uninitialized linked data structures**

997 Both kernel and userspace threads shall check the consistency of the previous and next pointers it manipulates when
998 adding or deleting an item to or from a linked list and reject the operation if they are not consistent.

999 **6.2.6.10 MI-CFIN: Control flow integrity**

1000 Both kernel and userspace threads shall protect saved function and return pointers from overwrite

1001 **6.2.6.11 MI-MPMT: Memory protection using memory tagging**

1002 Both kernel and userspace threads shall use hardware-supported memory tagging to reject erroneous memory accesses.

1003 **6.2.6.12 MI-MPUI: MPU-based task isolation**

1004 The product shall configure memory protection unit (MPU) regions to prevent each task from accessing the stack and
1005 private data of other tasks.

- 1006 • Applicability: Platform has a memory protection unit (MPU) and product runs multiple tasks

1007 **6.2.6.13 MI-STKG: Stack overflow detection and containment**

1008 The product shall detect stack overflow for every task and prevent the overflow from corrupting memory outside the
1009 overflowing task's stack region.

- 1010 • Applicability: Product runs multiple tasks with separate stack regions

1011 **6.2.7 TR-MINI: Minimize impact on other devices and services**

1012 **6.2.7.1 General**

1013 This clause groups mitigations that prevent the product from being abused to disrupt other devices or services on the
1014 network. Each mitigation defines its own verdict criteria.

1015 **6.2.7.2 MI-RRIS: Document residual risk to other devices and services**

1016 The product shall be accompanied by documentation describing the residual risk to other devices and services and the
1017 actions the user or the operational environment can take to mitigate it.

1018 **6.2.7.3 MI-MNET: Minimize negative impact of network transmission**

1019 The product shall minimise its negative impact on other products or services via the data it transmits on the network.
1020 Each source of network data shall be documented, along with the ways it can interfere with other products or services,
1021 and methods the product uses to minimise that interference.

1022 **6.2.7.4 MI-MAMP: Minimize negative impact of network traffic amplification**

1023 The product shall mitigate abuse of network services that amplify network traffic in manner that can be used to attack
1024 other devices. Each network service and its associated mitigations shall be documented.

1025 6.2.8 TR-SDEF: Secure by default configuration

1026 6.2.8.1 General

1027 This clause groups mitigations that establish a security baseline in the product's default configuration. It covers
1028 authorization controls on security-relevant assets and the protection or disablement of debug and management interfaces
1029 accessible by physical, local software, or network paths.

1030 6.2.8.2 MI-ADEF: Authorization required by default to access security-relevant assets

1031 The product, in its default state, shall require authentication and authorization for access to security-relevant assets. The
1032 authentication mechanism and the authorization rules applied to each class of security-relevant asset shall be
1033 documented by the manufacturer. For example, an autogenerated device-specific cryptographic key should not be
1034 readable without authentication and authorization.

- 1035 • Applicability: When the product is intended for integration into another product, the manufacturer shall
1036 document any security-relevant assets for which authentication and authorization are not enforced by the
1037 product itself and are expected to be provided by the integrator

1038 6.2.8.3 MI-PDDI-1: Document how to protect access to debug and management 1039 interfaces

1040 All debug and management interfaces on the product shall be documented, and the documentation shall specify means
1041 to protect or disable them.

- 1042 • Applicability: This mitigation is for products intended for integration into subsequent products.

1043 6.2.8.4 MI-PDDI-2: Protect or disable physical access to debug and management 1044 interfaces

1045 All debug and management interfaces which can be accessed by an agent with physical access to the device the product
1046 is installed on shall be protected or disabled by default, unless required for backward compatibility. Where the product
1047 allows the user to remove such protections, the manufacturer shall document the procedure, the residual risk, and the
1048 user roles permitted to perform the procedure.

1049 6.2.8.5 MI-PDDI-3: Protect or disable local software access to debug and management 1050 interfaces

1051 All debug and management interfaces which can be accessed by processes running on the system shall be protected or
1052 disabled by default, unless required for backward compatibility. Where the product allows the user to remove such
1053 protections, the manufacturer shall document the procedure, the residual risk, and the user roles permitted to perform
1054 the procedure.

1055 6.2.8.6 MI-PDDI-4: Protect or disable network access to debug or management 1056 interfaces

1057 All debug and management interfaces accessible via the network shall be protected or disabled by default, unless
1058 necessary for backward compatibility. Documentation regarding the removal of such protections by an appropriately
1059 sophisticated user may be provided, and shall include information regarding the risks.

1060 6.2.9 TR-SCUD: Secure updates

1061 6.2.9.1 General

1062 This clause addresses CRA Annex I, Part 1, (2)(c): products shall ensure that vulnerabilities can be addressed through
1063 security updates. It covers secure update documentation and delivery at first use (MI-KEVD, MI-KEVA), and the
1064 secure update mechanisms provided by the operational environment at three assurance levels (MI-SCHL, MI-SCHM,
1065 MI-SCHH). Security updates shall be delivered within the manufacturer's documented vulnerability remediation
1066 timeline. The product shall provide an opt-out mechanism that allows the user to postpone but not permanently disable
1067 security updates.

1068 A secure update mechanism shall provide at minimum: verification of the authenticity of the update source, verification
1069 of the integrity of the update package before installation, and protection of the update channel against interception or
1070 modification in transit.

1071 The assurance levels for secure updates provided by the operational environment are:

- 1072 • **Low:** the operational environment provides a method of notifying the user of available updates and a method
1073 of retrieving and applying them manually.
- 1074 • **Medium:** the operational environment provides authenticated notification of available updates, authenticated
1075 retrieval of updates, integrity verification of update packages before installation, and a method of applying
1076 them.
- 1077 • **High:** the operational environment provides all Medium-level properties and additionally provides automatic
1078 installation of security updates by default, with an opt-out mechanism that allows the user to postpone but not
1079 permanently disable updates.

1080 6.2.9.2 MI-KEVD: Documentation for secure update before or during first use

1081 The product shall be accompanied by documentation describing how the product may be securely updated, including
1082 how to update the product prior to, or as part of, first use.

- 1083 • Applicability: The product has firmware or software update capability

1084 6.2.9.3 MI-KEVA: Secure update before or during first use

1085 The product shall implement a secure update mechanism that operates by default before or during first use. The
1086 mechanism may be automatic or user-initiated provided that the product prompts the user to initiate the update before
1087 granting access to product functions.

- 1088 • Applicability: The product has firmware or software update capability

1089 6.2.9.4 MI-SCHL: Low security updates provided by operational environment

1090 The product shall be capable of receiving, verifying, and applying secure updates provided by the operational
1091 environment. The manufacturer shall document the requirements that the operational environment must satisfy to
1092 deliver secure updates at the Low assurance level.

1093 6.2.9.5 MI-SCHM: Medium security updates provided by operational environment

1094 The product shall be capable of receiving, verifying, and applying secure updates provided by the operational
1095 environment. The manufacturer shall document the requirements that the operational environment must satisfy to
1096 deliver secure updates at the Medium assurance level.

1097 6.2.9.6 MI-SCHH: High security updates provided by operational environment

1098 The product shall be capable of receiving, verifying, and applying secure updates provided by the operational
1099 environment. The manufacturer shall document the requirements that the operational environment must satisfy to
1100 deliver secure updates at the High assurance level.

1101 6.2.10 TR-AUTH: Authentication and access control

1102 6.2.10.1 General

1103 This clause groups mitigations for authentication and access control. It covers authentication of users and administrators
1104 on interfaces providing access to the operating system, authentication of peer endpoints at trust boundaries such as the
1105 boundary between the product and a remote data processing solution described in clause 4.8, authentication failure
1106 protection, protection of stored credentials and critical security parameters, enforcement of access control on operating-
1107 system resources, privilege separation where the operating system supports multiple privilege levels, and the lifecycle
1108 of authenticated sessions. Mitigations under this clause carry applicability fields that reflect the operating system's
1109 authentication model. Where a mitigation assumes a feature not provided by the operating system (for example,
1110 multiple privilege levels on a flat-privilege real-time operating system, or persistent sessions on an operating system
1111 that authenticates on each interaction), the applicability condition is not satisfied and the mitigation does not apply.
1112 Where cryptographic mechanisms are used to protect credentials or critical security parameters, cryptographic
1113 algorithms shall conform to TR-CRYP.

1114 **6.2.10.2 MI-RAUT: Authenticate the remote data processing solution at the RDPS**
 1115 **boundary**

1116 Where the product communicates with a remote data processing solution, the product shall authenticate the remote data
 1117 processing solution before transmitting data to it or acting upon interactions received from it that can influence the
 1118 behaviour, state, configuration, or security of a product function.

- 1119 • Applicability: Product depends on one or more remote data processing solutions

1120 **6.2.10.3 MI-AUTH: Require authentication on interfaces providing access to the**
 1121 **operating system**

1122 The operating system shall require user or administrator authentication on all interfaces that provide access to
 1123 operating-system resources or functions that are not intended for unauthenticated use.

- 1124 • Applicability: Product provides an interface that supports user or administrator authentication

1125 **6.2.10.4 MI-LCKT: Authentication failure protection**

1126 The operating system shall enforce authentication failure protection on each authentication interface, including (i)
 1127 progressive delays between failed attempts, and (ii) temporary account lockout after a configurable number of failed
 1128 attempts.

- 1129 • Applicability: Product provides an interface that supports user or administrator authentication

1130 **6.2.10.5 MI-CRED: Protect stored critical security parameters and enforce credential**
 1131 **entropy**

1132 The operating system shall protect stored credentials, cryptographic keys, and other critical security parameters using
 1133 mechanisms conforming to TR-CRYP, and shall enforce minimum credential entropy requirements documented by the
 1134 manufacturer for credentials it accepts through authentication interfaces.

- 1135 • Applicability: Product stores credentials, cryptographic keys, or other critical security parameters, or accepts
 1136 credentials through a user or administrator authentication interface

1137 **6.2.10.6 MI-ACCS: Access control enforcement on operating-system resources and**
 1138 **functions**

1139 The operating system shall enforce access control on operating-system resources and functions based on the
 1140 authenticated identity, role, privilege level, or other attributes of the requesting subject, as documented by the
 1141 manufacturer.

- 1142 • Applicability: Product supports differentiated access to operating-system resources or functions among
 1143 subjects

1144 **6.2.10.7 MI-PRIV: Privilege separation and restriction**

1145 Where the operating system supports multiple privilege levels, the operating system shall enforce privilege separation
 1146 between subjects executing at different privilege levels, and shall restrict each subject to the operations permitted at its
 1147 assigned privilege level.

- 1148 • Applicability: Product supports multiple privilege levels

1149 **6.2.10.8 MI-SESS: Session lifecycle controls**

1150 Where the operating system supports authenticated sessions that persist after initial authentication, the operating system
 1151 shall (i) invalidate each session after a configurable idle timeout period documented by the manufacturer, (ii) invalidate
 1152 each session immediately upon session logout or termination, upon authentication credential change, or upon timeout
 1153 expiration, and (iii) deny privilege escalation attempts within an active session without re-authentication or other
 1154 documented authorization.

- 1155 • Applicability: Product supports authenticated sessions that persist after initial authentication

1156 6.2.11 TR-CDST: Confidentiality of data stored on the product

1157 6.2.11.1 General

1158 This clause groups mitigations that protect the confidentiality of data stored on the product against unauthorized access.
1159 It covers protection mechanisms applied to stored data and the formal verification of those mechanisms where
1160 applicable. Where stored data is confidentiality-sensitive, the product applies a cryptographic encryption mechanism as
1161 described in clause [5.2.13](#).

1162 6.2.11.2 MI-CDST: Protect confidentiality of data stored on the product

1163 The product shall protect data stored on the product from unauthorized access.

1164 6.2.11.3 MI-FCST: Formal proof of enforcement of confidentiality of data stored on the 1165 product

1166 A formal proof, in a formal verification tool, shall demonstrate that the product protects data stored on the product from
1167 unauthorized access. The sufficiency of the formal verification tool, the formal definition of confidentiality, and the
1168 formal argument that it applies to a formalization of the product's source code shall be documented. The process to run
1169 the formal verification tool to produce a formal proof shall be documented.

1170 6.2.11.4 MI-ENST: Cryptographic encryption of stored data

1171 Where the product stores data for which unauthorized access would lead to a security incident, the product shall protect
1172 the confidentiality of that data at rest using a cryptographic encryption mechanism conforming to TR-CRYP.

- 1173 • Applicability: Product stores data whose unauthorized access would lead to a security incident

1174 6.2.12 TR-CDTX: Confidentiality of data transmitted by product

1175 6.2.12.1 General

1176 This clause groups mitigations that protect the confidentiality of data transmitted by the product against unauthorized
1177 access. It covers protection mechanisms applied to transmitted data and the documentation of any transfer of risk to the
1178 user. Where transmitted data is confidentiality-sensitive, the product applies a cryptographic encryption mechanism as
1179 described in clause [5.2.13](#).

1180 6.2.12.2 MI-CDTX: Protect confidentiality of data transmitted by product

1181 The product shall protect data transmitted by the product from unauthorized access.

1182 6.2.12.3 MI-RRDC: Document residual risk to confidentiality of data transmitted

1183 The product shall be accompanied by documentation describing the residual risk to the confidentiality of data
1184 transmitted by the product and the actions the user or the operational environment can take to mitigate it.

1185 6.2.12.4 MI-ENTX: Cryptographic encryption of transmitted data

1186 Where the product transmits data for which unauthorized disclosure would lead to a security incident, the product shall
1187 protect the confidentiality of that data in transit using a cryptographic encryption mechanism conforming to TR-CRYP.

- 1188 • Applicability: Product transmits data whose unauthorized disclosure would lead to a security incident

1189 6.2.13 TR-CRYP: Encryption

1190 6.2.13.1 General

1191 This clause groups mitigations that require the operating system to use state of the art cryptography for all
1192 cryptographic functions it provides to applications or uses internally, and that prohibit the use of deprecated or weak
1193 cryptography. Other clauses of the present document that depend on cryptographic mechanisms, including those
1194 covering confidentiality of stored and transmitted data, integrity of stored and transmitted data, authentication, secure
1195 updates, and boot integrity, rely on the requirements established in this clause.

1196 6.2.13.2 MI-CRYP: State of the art cryptography

1197 The product shall require state of the art cryptography for all cryptographic functions of the operating system, including
1198 cryptographic functions provided to applications through system libraries, kernel services, device drivers, and system-
1199 wide cryptographic policy configuration, and those used by the operating system for kernel module signature
1200 verification, boot integrity, and system random number generation. The product shall not enable deprecated or weak
1201 cryptography.

1202 6.2.14 TR-IDST: Integrity of data stored on the product

1203 6.2.14.1 General

1204 This clause groups mitigations that protect the integrity of data stored on the product against unauthorized modification
1205 and that detect corruption when it occurs. It covers protection mechanisms applied to stored data, corruption detection,
1206 and formal verification of integrity enforcement. Integrity may be protected by the environment, permissions,
1207 duplication, backups, or checksums. Where stored data is integrity-sensitive, the product applies a cryptographic
1208 integrity mechanism as described in clause [5.2.13](#).

1209 6.2.14.2 MI-IDST: Protect integrity of data stored on the product

1210 The product shall protect the integrity of data stored on the product from unauthorized modification.

1211 6.2.14.3 MI-DCST: Detect corruption of data stored

1212 The product shall detect corruption of the data stored on the product.

1213 6.2.14.4 MI-FIST: Formal proof of enforcement of integrity of data stored on the product

1214 A formal proof, in a formal verification tool, shall demonstrate that the product protects data stored on the product from
1215 unauthorized modification. The sufficiency of the formal verification tool, the formal definition of integrity, and the
1216 formal argument that it applies to a formalization of the product's source code shall be documented. The process to run
1217 the formal verification tool to produce a formal proof shall be documented.

1218 6.2.14.5 MI-INTS: Cryptographic integrity protection of stored data

1219 Where the product stores data for which unauthorized modification would lead to a security incident, the product shall
1220 protect the integrity of that data at rest using a cryptographic integrity mechanism conforming to TR-CRYP, such as a
1221 message authentication code or a digital signature.

- 1222 • Applicability: Product stores data whose unauthorized modification would lead to a security incident

1223 6.2.15 TR-IDTX: Integrity of data transmitted by the product

1224 6.2.15.1 General

1225 This clause groups mitigations that detect corruption of data transmitted by the product and that protect the integrity of
1226 transmitted data against unauthorized modification. Corruption may be detected by the environment, permissions,
1227 duplication, backups, or checksums. Where transmitted data is integrity-sensitive, the product applies a cryptographic
1228 integrity mechanism as described in clause [5.2.13](#).

1229 6.2.15.2 MI-DCTX: Detect corruption of data transmitted by the product

1230 The product shall detect corruption of the data transmitted by the product.

1231 6.2.15.3 MI-INTT: Cryptographic integrity protection of transmitted data

1232 Where the product transmits data for which unauthorized modification in transit would lead to a security incident, the
1233 product shall protect the integrity of that data using a cryptographic integrity mechanism conforming to TR-CRYP, such
1234 as a message authentication code or a digital signature.

- 1235 • Applicability: Product transmits data whose unauthorized modification in transit would lead to a security
1236 incident

1237 6.2.16 TR-DMIN: Data Minimization

1238 6.2.16.1 General

1239 This clause groups mitigations that limit the data processed by the product to what is necessary for its intended
1240 functions. It covers documentation and justification of the data the product processes.

1241 6.2.16.2 MI-DJST: Document and justify processed data

1242 All sources of data processed by the product in its secure-by-default configuration shall be documented. All sources of
1243 data processed shall have a documented rationale for why its processing is necessary for the functioning of the product
1244 in its secure-by-default configuration.

1245 6.2.17 TR-AVAI: Availability

1246 6.2.17.1 General

1247 This clause groups mitigations that protect the availability of the product's essential and core functions against denial-
1248 of-service conditions. It covers availability of network services, watchdog and self-recovery mechanisms, fast packet
1249 drop, memory and resource limits, fair resource scheduling, and documentation of risk transferred to the operational
1250 environment.

1251 6.2.17.2 MI-AVNT: Availability of network services

1252 The product shall protect the availability of essential and core network services through mitigation of denial-of-service
1253 attacks.

1254 6.2.17.3 MI-WDOG: Watchdog and self-initiated reset

1255 The product shall implement a mechanism to trigger an automatic reset when it detects that it is no longer able to
1256 perform its functions.

1257 6.2.17.4 MI-FDRP: Fast packet drop

1258 TODO: Write mitigation requiring the product to do validity checks on packets from both the network and the user in
1259 order of cheapest to most expensive so it can drop invalid packets with as little resource usage as possible.

1260 6.2.17.5 MI-LMEM: Limit memory usage

1261 TODO: Write mitigation requiring the product limit memory usage triggered by user input via network or local access.

1262 6.2.17.6 MI-FAIR: Fair resource usage and prioritization

1263 TODO: Write mitigation requiring the product implement some form of ensuring fair resource usage by multiple
1264 sources of input, including the ability to prioritize some sources of input.

1265 6.2.17.7 MI-RRDS: Document residual risk of denial of service

1266 The product shall be accompanied by documentation describing the residual risk of denial of service and the measures
1267 the operational environment can provide to mitigate it, such as an external or internal firewall, fair queueing or filtering,
1268 or a proxy.

1269 6.2.17.8 MI-RTDL: Real-time deadline preservation

1270 The product shall demonstrate that its security mechanisms do not cause the product to exceed documented worst-case
1271 execution times for real-time tasks.

- 1272 • Applicability: Product has documented real-time deadlines

1273 6.2.17.9 MI-RTRY: Retry and degraded behaviour on unavailability of the remote data 1274 processing solution

1275 Where the availability or timeliness of interactions with a remote data processing solution is necessary for the secure
1276 operation of the product, the product shall detect unavailability of the remote data processing solution or unacceptable
1277 delay of expected interactions, apply defined timeout controls for expected interactions, retry failed communications

1278 within 24 hours, and apply a defined behaviour for the dependent product function when the remote data processing
1279 solution remains unavailable beyond the acceptable time.

- 1280 • Applicability: Product depends on one or more remote data processing solutions

1281 6.2.18 TR-LMAS: Minimize exposed interfaces

1282 6.2.18.1 General

1283 This clause groups mitigations that minimize the interfaces exposed by the product in its default configuration, across
1284 all operating modes including initial configuration, initialization, runtime, shutdown, paused state, and reset. It covers
1285 documentation and justification of every interface that remains exposed.

1286 6.2.18.2 MI-JSTY: Document and justify exposed interfaces

1287 All exposed interfaces on the product in any state that is part of its reasonably foreseeable use or misuse in its secure-
1288 by-default configuration shall be documented. Every interface shall have a documented rationale for why its exposure is
1289 necessary for the functioning of the product in its secure-by-default configuration.

1290 6.2.19 TR-LOGG: Logging and monitoring

1291 6.2.19.1 General

1292 This clause groups mitigations that record security-relevant internal events of the product, including changes to
1293 configuration and access or modification of data, services or functions. It covers logging and the provision of an opt-out
1294 mechanism for the user.

1295 6.2.19.2 MI-LOGG: Logging

1296 The product shall support recording log messages for security-relevant events in accordance with the manufacturer's
1297 default secure configuration. The log messages shall not include any confidential information such as PII, secrets, or
1298 credentials, or any information which might reasonably be expected to include such items.

1299 6.2.20 TR-SCDL: Secure deletion

1300 6.2.20.1 General

1301 This clause groups mitigations that allow the user to delete all user data and settings from the product and return it to its
1302 default configuration. It covers secure deletion via reset, via reinstallation, and via dedicated deletion functions.
1303 Common secure deletion mechanisms include overwriting all user-writable storage, or encrypting user data and deleting
1304 the key.

1305 6.2.20.2 MI-RSET: Secure deletion via reset

1306 The product shall reset to its secure-by-default state after a power cycle or reset command.

- 1307 • Applicability: Product has the capability for the user to write data and/or settings

1308 6.2.20.3 MI-INST: Secure deletion via reinstallation

1309 The product shall reset to its secure-by-default state after a reinstallation that securely deletes all previous user data or
1310 settings.

- 1311 • Applicability: Product has the capability for the user to write data and/or settings

1312 6.2.20.4 MI-DELE: Secure deletion via secure deletion function

1313 The product shall reset to its secure-by-default state after the secure deletion function is used.

1314 NOTE: Editor's Note: this section should be clarified so that the method of deletion depends upon the sensitivity
1315 of data stored.

- 1316 • Applicability: Product has the capability for the user to write data and/or settings

1317 6.2.21 TR-SDTR: Secure data read and transfer

1318 6.2.21.1 General

1319 This clause groups mitigations that allow the user to read all data and settings from the product and, where supported,
1320 transfer them securely to another product. It covers data read and data transfer mechanisms.

1321 6.2.21.2 MI-SDRF: Secure data read from product

1322 The product shall provide a method by which an authorized user can securely read all data and settings from the
1323 product.

- 1324 • Applicability: Product has the capability for the user to write data and/or settings

1325 6.2.21.3 MI-SDTR: Secure data transfer to another product

1326 If the product provides a method to transfer data and settings to another product, it shall do so securely.

- 1327 • Applicability: Product has the capability for the user to write data and/or settings and to transfer them to
1328 another product.

1329 6.2.22 TR-VULH: Vulnerability handling

1330 6.2.22.1 General

1331 This clause addresses CRA Annex I, Part 2: vulnerability handling. The horizontal standard [2] prEN 40000-1-3 defines
1332 the vulnerability handling processes that apply to all products with digital elements, including SBOM requirements.
1333 This clause does not duplicate those requirements. For end-user operating system products, vulnerability handling is
1334 assessed entirely under [2] prEN 40000-1-3. For operating systems intended for integration into subsequent products,
1335 MI-VULH-1 adds the obligation to share SBOM details with downstream manufacturers to enable coordinated
1336 vulnerability handling.

1337 6.2.22.2 MI-VULH-1: Enabling Vulnerability Handling in Integrated Products

1338 When the product is intended for integration into subsequent products in a supply chain, system vulnerabilities may
1339 have a particularly high impact on the security characteristics of the final product. Therefore, manufacturers of
1340 operating systems intended for integration in subsequent products have a responsibility to enable the vulnerability
1341 handling processes of manufacturers which depend upon them. This is accomplished by sharing details of the operating
1342 system's components to enable downstream manufacturers to participate in coordinated vulnerability handling
1343 procedures described in [2] prEN 40000-1-3 "Cybersecurity requirements for products with digital elements -
1344 Vulnerability Handling".

- 1345 • Applicability: any operating system intended for integration in subsequent products, rather than use by an end-
1346 user

1347 6.3 Risk Mitigation Sets

1348 6.3.1 General

1349 The security profiles in this clause are the normative basis for determining which mitigations a product shall implement.
1350 Each security profile corresponds to one or more use cases described in clause [4.7](#). The derivation of security profiles
1351 from risk factors and threat assessments is described in Annex B.

1352 A product shall implement every mitigation listed under its applicable security profile. Where a mitigation also carries
1353 an applicability field, that mitigation applies only when the stated condition holds for the product.

1354 Where a security profile lists alternative mitigations separated by “or”, the manufacturer shall implement at least one of
1355 the listed alternatives. The selection shall be based on the product’s implementation characteristics and capabilities. For
1356 example, (SSCA or FVFC) allows the manufacturer to choose static source code analysis or formal verification. (FZ95
1357 or BTIN or IMSL) allows runtime coverage testing, boundary testing, or implementation in a memory-safe language.
1358 (KEVT or SCAN) allows manual vulnerability testing or automated scanning. (RRIS or MAMP) allows documenting
1359 residual risk or actively mitigating traffic amplification. The manufacturer shall document which alternative was
1360 selected and the rationale for the selection, as part of the conformity assessment evidence.

1361 6.3.2 SP-LR required mitigations

1362 This profile represents products with all risk factors at level 0, meaning no network exposure, no user accounts, no
 1363 sensitive data or functions, no physical exposure, and no untrusted inputs. The risk assessment in Annex B evaluates
 1364 every threat's likelihood and impact as Low without additional mitigations. Products assigned to this profile remain
 1365 subject to the CRA essential requirements and to the vulnerability handling requirements of the horizontal standard [2]
 1366 prEN 40000-1-3.

1367 None.

1368 6.3.3 SP-IoT-1 required mitigations

1369 This profile represents low-risk IoT products with risk factors at level 0 except for administration by unskilled
 1370 administrators. The risk assessment in Annex B evaluates every threat's likelihood and impact as Low without
 1371 additional mitigations. Products assigned to this profile remain subject to the CRA essential requirements and to the
 1372 vulnerability handling requirements of the horizontal standard [2] prEN 40000-1-3.

1373 None.

1374 6.3.4 SP-IoT-2 required mitigations

1375 1. (SSCA or FVFC)

1376 2. SCFS

1377 3. MMAC

1378 4. ADEF

1379 5. LOGG

1380 6. KEVA

1381 7. KEVM

1382 8. (KEVT or SCAN)

1383 9. (SUAP or SUA0)

1384 10. VULH

1385 11. PDDI-1

1386 12. AUTH

1387 13. RAUT

1388 14. RTRY

1389 15. LCKT

1390 16. CRED

1391 17. ACCS

1392 18. PRIV

1393 19. SESS

1394 20. RRDC

1395 21. DJST

1396 22. RRDS

1397 23. (RRIS or MAMP)

1398 24. SUDC

1399	25. CDTX
1400	26. ENTX
1401	27. CRYP
1402	28. IDTX
1403	29. INTT
1404	30. DMIN

1405 6.3.5 SP-IoT-3 required mitigations

1406	1. (SSCA or FVFC)
1407	2. SCFS
1408	3. MMAC
1409	4. ADEF
1410	5. LOGG
1411	6. KEVA
1412	7. KEVM
1413	8. (KEVT or SCAN)
1414	9. (SUAP or SUA0)
1415	10. VULH
1416	11. PDDI-1
1417	12. AUTH
1418	13. RAUT
1419	14. RTRY
1420	15. LCKT
1421	16. CRED
1422	17. ACCS
1423	18. PRIV
1424	19. SESS
1425	20. RRDC
1426	21. DJST
1427	22. RRDS
1428	23. LMEM
1429	24. (RRIS or MAMP)
1430	25. SUDC
1431	26. CDTX
1432	27. ENTX
1433	28. CRYP

- 1434 29. IDTX
- 1435 30. INTT
- 1436 31. DMIN

1437 6.3.6 SP-RO-1 required mitigations

- 1438 1. (SSCA or FVFC)
- 1439 2. (FZ95 or BTIN or IMSL)
- 1440 3. SCFS
- 1441 4. MMAC
- 1442 5. ASLR
- 1443 6. MSAF-*
- 1444 7. MZRO-*
- 1445 8. MRWX-*
- 1446 9. NKAM
- 1447 10. PULS
- 1448 11. MRCO
- 1449 12. MPUI
- 1450 13. STKG
- 1451 14. ADEF
- 1452 15. JSTY
- 1453 16. LOGG
- 1454 17. KEVA
- 1455 18. KEVM
- 1456 19. (KEVT or SCAN)
- 1457 20. (SUAP or SUA0)
- 1458 21. VULH
- 1459 22. PDDI-1
- 1460 23. PDDI-4
- 1461 24. AUTH
- 1462 25. LCKT
- 1463 26. CRED
- 1464 27. ACCS
- 1465 28. PRIV
- 1466 29. SESS
- 1467 30. CDTX
- 1468 31. ENTX

1469	32. DCTX
1470	33. RRDC
1471	34. DJST
1472	35. RRDS
1473	36. AVNT
1474	37. FDRP
1475	38. LMEM
1476	39. FAIR
1477	40. RTDL
1478	41. MNET
1479	42. MAMP
1480	43. SUDC
1481	44. CRYP
1482	45. IDTX
1483	46. INTT
1484	47. DMIN

1485 6.3.7 SP-OT-1 required mitigations

1486	1. (SSCA or FVFC)
1487	2. (FZ95 or BTIN or IMSL)
1488	3. SCFS
1489	4. MMAC
1490	5. ASLR
1491	6. MSAF-*
1492	7. MZRO-*
1493	8. MRWX-*
1494	9. NKAM
1495	10. PULS
1496	11. MRCO
1497	12. MPUI
1498	13. STKG
1499	14. ADEF
1500	15. JSTY
1501	16. LOGG
1502	17. KEVA
1503	18. KEVM

- 1504 19. (KEVT or SCAN)
- 1505 20. (SUAP or SUA0)
- 1506 21. VULH
- 1507 22. PDDI-1
- 1508 23. PDDI-2
- 1509 24. PDDI-4
- 1510 25. AUTH
- 1511 26. LCKT
- 1512 27. CRED
- 1513 28. ACCS
- 1514 29. PRIV
- 1515 30. SESS
- 1516 31. RRDC
- 1517 32. DJST
- 1518 33. RRDS
- 1519 34. AVNT
- 1520 35. FDRP
- 1521 36. LMEM
- 1522 37. FAIR
- 1523 38. RTDL
- 1524 39. (RRIS or MAMP)
- 1525 40. SUDC
- 1526 41. CDTX
- 1527 42. ENTX
- 1528 43. CRYP
- 1529 44. IDTX
- 1530 45. INTT
- 1531 46. DMIN

1532 6.3.8 SP-MOB-1 required mitigations

- 1533 1. (SSCA or FVFC)
- 1534 2. (FZ95 or BTIN or IMSL)
- 1535 3. SCFS
- 1536 4. MMAC
- 1537 5. ASLR
- 1538 6. MSAF-*

1539	7. MZRO-*
1540	8. MRWX-*
1541	9. NKAM
1542	10. PULS
1543	11. MRCO
1544	12. MPUI
1545	13. STKG
1546	14. ADEF
1547	15. JSTY
1548	16. LOGG
1549	17. KEVA
1550	18. KEVM
1551	19. (KEVT or SCAN)
1552	20. (SUAP or SUA0)
1553	21. VULH
1554	22. PDDI-2
1555	23. PDDI-4
1556	24. AUTH
1557	25. LCKT
1558	26. CRED
1559	27. ACCS
1560	28. PRIV
1561	29. SESS
1562	30. CDTX
1563	31. ENTX
1564	32. DCTX
1565	33. RRDC
1566	34. DJST
1567	35. RRDS
1568	36. AVNT
1569	37. FDRP
1570	38. LMEM
1571	39. FAIR
1572	40. RTDL
1573	41. MNET

- 1574 42. MAMP
- 1575 43. SUDC
- 1576 44. CRYP
- 1577 45. IDTX
- 1578 46. INTT
- 1579 47. DMIN

1580 6.3.9 SP-WE-1 required mitigations

- 1581 1. (SSCA or FVFC)
- 1582 2. SCFS
- 1583 3. MMAC
- 1584 4. ADEF
- 1585 5. JSTY
- 1586 6. LOGG
- 1587 7. (KEVD or KEVA)
- 1588 8. KEVM
- 1589 9. (SUVF or SUAP or SUOE or SUAQ)
- 1590 10. VULH
- 1591 11. PDDI-1
- 1592 12. PDDI-2
- 1593 13. PDDI-4
- 1594 14. AUTH
- 1595 15. RAUT
- 1596 16. RTRY
- 1597 17. LCKT
- 1598 18. CRED
- 1599 19. ACCS
- 1600 20. PRIV
- 1601 21. SESS
- 1602 22. RRDC
- 1603 23. DJST
- 1604 24. RRDS
- 1605 25. (RRIS or MAMP)
- 1606 26. SUDC
- 1607 27. CDTX
- 1608 28. ENTX

- 1609 29. CRYP
- 1610 30. IDTX
- 1611 31. INTT
- 1612 32. DMIN

1613 6.3.10 SP-PC-1 required mitigations

- 1614 1. (SSCA or FVFC)
- 1615 2. (FZ95 or BTIN or IMSL)
- 1616 3. SCFS
- 1617 4. MMAC
- 1618 5. ASLR
- 1619 6. MSAF-*
- 1620 7. MZRO-*
- 1621 8. MRWX-*
- 1622 9. NKAM
- 1623 10. PULS
- 1624 11. MRCO
- 1625 12. MPUI
- 1626 13. STKG
- 1627 14. ADEF
- 1628 15. JSTY
- 1629 16. LOGG
- 1630 17. KEVA
- 1631 18. KEVM
- 1632 19. (KEVT or SCAN)
- 1633 20. (SUAP or SUA0)
- 1634 21. VULH
- 1635 22. PDDI-1
- 1636 23. PDDI-3
- 1637 24. PDDI-4
- 1638 25. AUTH
- 1639 26. LCKT
- 1640 27. CRED
- 1641 28. ACCS
- 1642 29. PRIV
- 1643 30. SESS

1644	31. CDTX
1645	32. ENTX
1646	33. DCTX
1647	34. RRDC
1648	35. DJST
1649	36. RRDS
1650	37. LMEM
1651	38. MNET
1652	39. MAMP
1653	40. SUDC
1654	41. CRYP
1655	42. IDTX
1656	43. INTT
1657	44. DMIN

1658 6.3.11 SP-PC-2 required mitigations

1659	1. (SSCA or FVFC)
1660	2. (FZ95 or BTIN or IMSL)
1661	3. SCFS
1662	4. MMAC
1663	5. ASLR
1664	6. MSAF-*
1665	7. MZRO-*
1666	8. MRWX-*
1667	9. NKAM
1668	10. PULS
1669	11. MRCO
1670	12. MPUI
1671	13. STKG
1672	14. ADEF
1673	15. JSTY
1674	16. LOGG
1675	17. KEVA
1676	18. KEVM
1677	19. (KEVT or SCAN)
1678	20. (SUAP or SUA0)

1679	21. VULH
1680	22. PDDI-1
1681	23. PDDI-3
1682	24. PDDI-4
1683	25. AUTH
1684	26. LCKT
1685	27. CRED
1686	28. ACCS
1687	29. PRIV
1688	30. SESS
1689	31. CDTX
1690	32. ENTX
1691	33. DCTX
1692	34. RRDC
1693	35. DJST
1694	36. RRDS
1695	37. AVNT
1696	38. FDRP
1697	39. LMEM
1698	40. FAIR
1699	41. RTDL
1700	42. MNET
1701	43. MAMP
1702	44. SUDC
1703	45. CRYP
1704	46. IDTX
1705	47. INTT
1706	48. DMIN

1707 6.3.12 SP-LA-1 required mitigations

1708	1. (SSCA or FVFC)
1709	2. (FZ95 or BTIN or IMSL)
1710	3. SCFS
1711	4. MMAC
1712	5. ASLR
1713	6. MSAF-*

1714	7. MZRO-*
1715	8. MRWX-*
1716	9. NKAM
1717	10. PULS
1718	11. MRCO
1719	12. MPUI
1720	13. STKG
1721	14. ADEF
1722	15. JSTY
1723	16. LOGG
1724	17. KEVA
1725	18. KEVM
1726	19. (KEVT or SCAN)
1727	20. (SUAP or SUA0)
1728	21. VULH
1729	22. PDDI-2
1730	23. PDDI-3
1731	24. PDDI-4
1732	25. AUTH
1733	26. LCKT
1734	27. CRED
1735	28. ACCS
1736	29. PRIV
1737	30. SESS
1738	31. CDTX
1739	32. ENTX
1740	33. DCTX
1741	34. RRDC
1742	35. DJST
1743	36. RRDS
1744	37. LMEM
1745	38. MNET
1746	39. MAMP
1747	40. SUDC
1748	41. CRYP

- 1749 42. IDTX
- 1750 43. INTT
- 1751 44. DMIN

1752 6.3.13 SP-LA-2 required mitigations

- 1753 1. (SSCA or FVFC)
- 1754 2. (FZ95 or BTIN or IMSL)
- 1755 3. SCFS
- 1756 4. MMAC
- 1757 5. ASLR
- 1758 6. MSAF-*
- 1759 7. MZRO-*
- 1760 8. MRWX-*
- 1761 9. NKAM
- 1762 10. PULS
- 1763 11. MRCO
- 1764 12. MPUI
- 1765 13. STKG
- 1766 14. ADEF
- 1767 15. JSTY
- 1768 16. LOGG
- 1769 17. KEVA
- 1770 18. KEVM
- 1771 19. (KEVT or SCAN)
- 1772 20. (SUAP or SUA0)
- 1773 21. VULH
- 1774 22. PDDI-2
- 1775 23. PDDI-3
- 1776 24. PDDI-4
- 1777 25. AUTH
- 1778 26. LCKT
- 1779 27. CRED
- 1780 28. ACCS
- 1781 29. PRIV
- 1782 30. SESS
- 1783 31. CDTX

1784	32. ENTX
1785	33. DCTX
1786	34. RRDC
1787	35. DJST
1788	36. RRDS
1789	37. AVNT
1790	38. FDRP
1791	39. LMEM
1792	40. FAIR
1793	41. RTDL
1794	42. MNET
1795	43. MAMP
1796	44. SUDC
1797	45. CRYP
1798	46. IDTX
1799	47. INTT
1800	48. DMIN

1801 6.3.14 SP-PS-1 required mitigations

1802	1. (SSCA or FVFC)
1803	2. (FZ95 or BTIN or IMSL)
1804	3. SCFS
1805	4. MMAC
1806	5. ASLR
1807	6. MSAF-*
1808	7. MZRO-*
1809	8. MRWX-*
1810	9. NKAM
1811	10. PULS
1812	11. MRCO
1813	12. MPUI
1814	13. STKG
1815	14. ADEF
1816	15. JSTY
1817	16. LOGG
1818	17. KEVA

- 1819 18. KEVM
- 1820 19. (KEVT or SCAN)
- 1821 20. (SUAP or SUA0)
- 1822 21. VULH
- 1823 22. PDDI-1
- 1824 23. PDDI-3
- 1825 24. PDDI-4
- 1826 25. AUTH
- 1827 26. LCKT
- 1828 27. CRED
- 1829 28. ACCS
- 1830 29. PRIV
- 1831 30. SESS
- 1832 31. CDTX
- 1833 32. ENTX
- 1834 33. DCTX
- 1835 34. RRDC
- 1836 35. DJST
- 1837 36. RRDS
- 1838 37. LMEM
- 1839 38. MNET
- 1840 39. MAMP
- 1841 40. SUDC
- 1842 41. CRYP
- 1843 42. IDTX
- 1844 43. INTT
- 1845 44. (RRMD or PMSC)
- 1846 45. DMIN

1847 6.3.15 SP-SE-1 required mitigations

- 1848 1. (SSCA or FVFC)
- 1849 2. (FZ95 or BTIN or IMSL)
- 1850 3. SCFS
- 1851 4. MMAC
- 1852 5. ASLR
- 1853 6. MSAF-*

1854	7. MZRO-*
1855	8. MRWX-*
1856	9. NKAM
1857	10. PULS
1858	11. MRCO
1859	12. MPUI
1860	13. STKG
1861	14. ADEF
1862	15. JSTY
1863	16. LOGG
1864	17. KEVA
1865	18. KEVM
1866	19. (KEVT or SCAN)
1867	20. (SUAP or SUA0)
1868	21. VULH
1869	22. PDDI-1
1870	23. PDDI-3
1871	24. PDDI-4
1872	25. AUTH
1873	26. LCKT
1874	27. CRED
1875	28. ACCS
1876	29. PRIV
1877	30. SESS
1878	31. CDTX
1879	32. ENTX
1880	33. DCTX
1881	34. RRDC
1882	35. DJST
1883	36. RRDS
1884	37. AVNT
1885	38. FDRP
1886	39. LMEM
1887	40. FAIR
1888	41. RTDL

- 1889 42. MNET
- 1890 43. MAMP
- 1891 44. SUDC
- 1892 45. CRYP
- 1893 46. IDTX
- 1894 47. INTT
- 1895 48. DMIN

1896 6.3.16 SP-SE-2 required mitigations

- 1897 1. (SSCA or FVFC)
- 1898 2. (FZ95 or BTIN or IMSL)
- 1899 3. SCFS
- 1900 4. MMAC
- 1901 5. ASLR
- 1902 6. MSAF-*
- 1903 7. MZRO-*
- 1904 8. MRWX-*
- 1905 9. NKAM
- 1906 10. PULS
- 1907 11. MRCO
- 1908 12. MPUI
- 1909 13. STKG
- 1910 14. ADEF
- 1911 15. JSTY
- 1912 16. LOGG
- 1913 17. KEVA
- 1914 18. KEVM
- 1915 19. (KEVT or SCAN)
- 1916 20. (SUAP or SUA0)
- 1917 21. VULH
- 1918 22. PDDI-1
- 1919 23. PDDI-3
- 1920 24. PDDI-4
- 1921 25. AUTH
- 1922 26. LCKT
- 1923 27. CRED

1924	28. ACCS
1925	29. PRIV
1926	30. SESS
1927	31. CDTX
1928	32. ENTX
1929	33. DCTX
1930	34. RRDC
1931	35. DJST
1932	36. RRDS
1933	37. AVNT
1934	38. FDRP
1935	39. LMEM
1936	40. FAIR
1937	41. RTDL
1938	42. MNET
1939	43. MAMP
1940	44. SUDC
1941	45. CRYP
1942	46. IDTX
1943	47. INTT
1944	48. (RRMD or PMSC)
1945	49. DMIN

1946 6.3.17 SP-SE-3 required mitigations

1947	1. (SSCA or FVFC)
1948	2. (FZ95 or BTIN or IMSL)
1949	3. SCFS
1950	4. MMAC
1951	5. ASLR
1952	6. MSAF-*
1953	7. MZRO-*
1954	8. MRWX-*
1955	9. NKAM
1956	10. PULS
1957	11. MRCO
1958	12. MPUI

1959	13. STKG
1960	14. ADEF
1961	15. JSTY
1962	16. LOGG
1963	17. KEVA
1964	18. KEVM
1965	19. (KEVT or SCAN)
1966	20. (SUAP or SUA0)
1967	21. VULH
1968	22. PDDI-1
1969	23. PDDI-3
1970	24. PDDI-4
1971	25. AUTH
1972	26. LCKT
1973	27. CRED
1974	28. ACCS
1975	29. PRIV
1976	30. SESS
1977	31. CDTX
1978	32. ENTX
1979	33. DCTX
1980	34. RRDC
1981	35. DJST
1982	36. RRDS
1983	37. AVNT
1984	38. FDRP
1985	39. LMEM
1986	40. FAIR
1987	41. RTDL
1988	42. MNET
1989	43. MAMP
1990	44. SUDC
1991	45. CRYP
1992	46. IDTX
1993	47. INTT

1994 48. (RRMD or PMSC)

1995 49. DMIN

1996

1997	7	Conformity assessment
1998	7.1	General
1999		This clause details the assessment process for compliance with the requirements in clause 5 of the present document.
2000		Each assessment activity in this clause corresponds to a mitigation in clause 5.2.
2001		NOTE: In this clause, <i>documentation</i> means any documentation provided to the assessor. This includes, but is not
2002		limited to, the technical specification, test results, and instructions to the user.
2003	7.2	TR-NKEV: No known exploitable vulnerabilities at first use
2004		[AC-KEVM] Assessment criteria: Documentation of mitigation of known exploitable vulnerabilities
2005		Assessment reference
2006		Mitigation MI-KEVM .
2007		Assessment objective
2008		Prevent exploitation of known exploitable vulnerabilities at first use
2009		Assessment preparation
2010		1. Compile a list of known exploitable vulnerabilities in the product's kernel, system libraries, device drivers, pre-
2011		installed applications, and any package management system, by consulting public vulnerability databases (such
2012		as CVE, NVD), upstream security advisories from component maintainers, and the manufacturer's own
2013		vulnerability records
2014		Assessment activities
2015		1. Compare the generated list of known exploitable vulnerabilities with the manufacturer's documentation of
2016		remediated and outstanding vulnerabilities
2017		Assessment verdict
2018		The verdict fail is assigned if any of the following conditions apply:
2019		1. Any known exploitable vulnerability is neither remediated nor documented with the residual risk and any
2020		compensating control, or any vulnerability exceeds the manufacturer's documented vulnerability remediation
2021		timeline without documented justification
2022		The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
2023		1. No known exploitable vulnerabilities found, or all reported vulnerabilities are either remediated or documented
2024		with the residual risk and any compensating control within the manufacturer's documented vulnerability
2025		remediation timeline
2026		Assessment evidence
2027		1. Documented vulnerability handling policy, list of known exploitable vulnerabilities, documentation of
2028		remediation or residual risk for each vulnerability, correlation of the list with the manufacturer's records
2029		
2030		[AC-KEVT] Assessment criteria: Testing for known exploitable vulnerabilities
2031		Assessment reference
2032		Mitigation MI-KEVT .
2033		Assessment objective
2034		Prevent exploitation of known exploitable vulnerabilities at first use
2035		Assessment preparation
2036		1. Compile a list of known exploitable vulnerabilities in the product and its components by consulting public
2037		vulnerability databases (such as CVE, NVD) and the manufacturer's own vulnerability records

- 2038 2. Select the vulnerabilities to be tested, prioritising by severity, known exploitation in the wild, impact on the
 2039 product, and privilege escalation potential
 2040 3. Collect or prepare test procedures for each selected vulnerability

2041 **Assessment activities**

- 2042 1. On a new product, run the tests and compare the results with the generated list of known exploitable
 2043 vulnerabilities

2044 **Assessment verdict**

2045 The verdict fail is assigned if any of the following conditions apply:

- 2046 1. Any tested vulnerability is not mitigated, or any untested vulnerability lacks documentation of the residual risk
 2047 and any compensating control

2048 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2049 1. No known exploitable vulnerabilities found, or all tested vulnerabilities are mitigated, and any untested
 2050 vulnerabilities are documented with the residual risk and any compensating control

2051 **Assessment evidence**

- 2052 1. Documented vulnerability handling policy, list of known exploitable vulnerabilities, test selection rationale,
 2053 test results for each tested vulnerability, documentation of residual risk for any untested vulnerability
 2054

2055 [\[AC-SCAN\]](#) Assessment criteria: No scannable known exploitable vulnerabilities

2056 **Assessment reference**

2057 Mitigation [MI-SCAN](#).

2058 **Assessment objective**

2059 Prevent exploitation of known exploitable vulnerabilities at first use

2060 **Assessment preparation**

- 2061 1. Select a set of automated vulnerability scanners documented by the manufacturer for the product

2062 **Assessment activities**

- 2063 1. On a new product, run the selected scanners and examine the documentation for any reported vulnerabilities

2064 **Assessment verdict**

2065 The verdict fail is assigned if any of the following conditions apply:

- 2066 1. Any reported vulnerability lacks documentation of the disposition, residual risk, or any compensating control

2067 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2068 1. No vulnerabilities found, or all reported vulnerabilities are documented with the disposition, residual risk, and
 2069 any compensating control

2070 **Assessment evidence**

- 2071 1. Documented vulnerability handling policy, list of vulnerability scanners selected, reports from each scanner,
 2072 correlation of reports with documentation of dispositions
 2073

2074 **7.3 TR-SSDD: Secure software design and development**

2075 [\[AC-SSCA\]](#) Assessment criteria: Static source code analysis for memory errors in memory unsafe languages

2076 **Assessment reference**

2077 Mitigation [MI-SSCA](#).

2078 **Assessment objective**

2079 Prevent unauthorized memory access

2080 **Assessment activities**

2081 1. Review the tool selection and configuration criteria documented by the manufacturer, the source code for the
2082 product, the output of the source code analysis tool, and the documentation for any warnings or suppression of
2083 warnings

2084 **Assessment verdict**

2085 The verdict fail is assigned if any of the following conditions apply:

2086 1. The tool selection or configuration criteria are not documented, the criteria do not cover the listed memory
2087 error classes, the tool output is not consistent with the source code, or any warning, annotation, or suppression
2088 lacks documentation of the residual risk and any compensating control

2089 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

2090 1. The tool selection and configuration criteria are documented, the criteria cover the listed memory error classes,
2091 the tool output is consistent with the source code, and each warning, annotation, or suppression is documented
2092 with the residual risk and any compensating control

2093 **Assessment evidence**

2094 1. The documentation documenting the tool selection and configuration criteria, how the tool is run, the source
2095 code for the product, the output of the source code analysis tool, and the documentation for any warnings or
2096 suppression of warnings
2097

2098 [\[AC-FZ95\]](#) Assessment criteria: Runtime code coverage checking with memory access error detection

2099 **Assessment reference**

2100 Mitigation [MI-FZ95](#).

2101 **Assessment objective**

2102 Prevent unauthorized memory access

2103 **Assessment activities**

2104 1. Run the tool while measuring statement coverage and monitoring for memory access errors until 95%
2105 statement coverage has been reached

2106 **Assessment verdict**

2107 The verdict fail is assigned if any of the following conditions apply:

2108 1. Statement coverage was less than 95%, or any reported memory error was neither remediated nor documented
2109 with the residual risk and any compensating control

2110 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

2111 1. Statement coverage was at least 95%, and each reported memory error was either remediated or documented
2112 with the residual risk and any compensating control

2113 **Assessment evidence**

2114 1. Logs of statement coverage tool, memory error report, documentation of any memory errors
2115

2116 [\[AC-IMSL\]](#) Assessment criteria: Implement in a memory-safe language

2117 **Assessment reference**

2118 Mitigation [MI-IMSL](#).

2119 **Assessment objective**

2120 Prevent unauthorized memory access

2121 **Assessment activities**

- 2122 1. Review source code to determine its language and what exceptions to memory safety exist
- 2123 **Assessment verdict**
- 2124 The verdict fail is assigned if any of the following conditions apply:
- 2125 1. Source code is not in a memory-safe language, or any use of unsafe memory features is not documented with
2126 the residual risk and any compensating control
- 2127 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
- 2128 1. Source code is in a memory-safe language and each use of unsafe memory features is documented with the
2129 residual risk and any compensating control
- 2130 **Assessment evidence**
- 2131 1. Source code, documentation of unsafe memory features
2132
- 2133 [\[AC-BTIN\]](#) Assessment criteria: Boundary testing of inputs that may cause memory errors
- 2134 **Assessment reference**
- 2135 Mitigation [MI-BTIN](#).
- 2136 **Assessment objective**
- 2137 Prevent unauthorized memory access
- 2138 **Assessment preparation**
- 2139 1. Identify input fields in the product that may produce memory errors
- 2140 **Assessment activities**
- 2141 1. Run a tool that tests the boundaries of the input values (minimum valid, maximum valid, minimum possible,
2142 maximum possible, off-by-one, etc.) while monitoring for memory errors
- 2143 **Assessment verdict**
- 2144 The verdict fail is assigned if any of the following conditions apply:
- 2145 1. Any boundary value was not tested, or any detected memory error was neither remediated nor documented
2146 with the residual risk and any compensating control
- 2147 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
- 2148 1. All boundary values were tested, and each detected memory error was either remediated or documented with
2149 the residual risk and any compensating control
- 2150 **Assessment evidence**
- 2151 1. Logs of boundary testing tool, memory error report, documentation of any memory errors
2152
- 2153 [\[AC-SCFS\]](#) Assessment criteria: Secure compilation flags
- 2154 **Assessment reference**
- 2155 Mitigation [MI-SCFS](#).
- 2156 **Assessment objective**
- 2157 Secure software design and development
- 2158 **Assessment preparation**
- 2159 1. Document which flags should be used
- 2160 **Assessment activities**
- 2161 1. Review compilation flags, warnings, and documentation for exceptions
- 2162 **Assessment verdict**

2163 The verdict fail is assigned if any of the following conditions apply:

- 2164 1. Documentation of flags does not exist, or any warning or exception is not documented

2165 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2166 1. Documentation of flags exists, all warnings and exceptions are documented

2167 **Assessment evidence**

- 2168 1. Documentation of flags, build system files, documentation of warnings and exceptions

2169

2170 [\[AC-FVFC\]](#) Assessment criteria: Formal verification of functional correctness

2171 **Assessment reference**

2172 Mitigation [MI-FVFC](#).

2173 **Assessment objective**

2174 Ensure the operating system source code behaves precisely as its specification mandates (potentially including
2175 prevention of unauthorized memory access)

2176 **Assessment activities**

- 2177 1. Review the tool selection and configuration criteria documented by the manufacturer, the source code for the
2178 product, the formal specification of the product, and (depending on the formal verification tool used) the
2179 output proof of the formal verification tool.

2180 **Assessment verdict**

2181 The verdict fail is assigned if any of the following conditions apply:

- 2182 1. The tool selection or configuration criteria are not documented, the formal specification is not a complete
2183 abstract description of the product, or the formal verification tool does not successfully output a proof of
2184 conformity

2185 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2186 1. The tool selection and configuration criteria are documented, the formal specification is a complete abstract
2187 description of the product, the formal verification tool successfully outputs a proof of conformity between the
2188 source code and the specification

2189 **Assessment evidence**

- 2190 1. The documentation documenting the tool selection and configuration criteria, how the tool is run, the source
2191 code for the product, the formal specification of the product, and (if applicable for the chosen formal
2192 verification tool) the output proof of the formal verification tool.

2193

2194 7.4 TR-MISO: Prevent local unauthorized access of memory- 2195 addressable security-relevant data

2196 [\[AC-MMAC\]](#) Assessment criteria: Memory access control

2197 **Assessment reference**

2198 Mitigation [MI-MMAC](#).

2199 **Assessment objective**

2200 Prevent unauthorized memory access

2201 **Assessment preparation**

- 2202 1. List the methods of accessing memory and the types of access control to memory

2203 **Assessment activities**

2204 1. For each method of accessing memory and each type of access control to memory, attempt to use the method
 2205 of accessing memory to gain access to memory that the executable is not authorized to access due to the access
 2206 control

2207 **Assessment verdict**

2208 The verdict fail is assigned if any of the following conditions apply:

2209 1. Any memory access succeeds

2210 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

2211 1. All memory accesses fail

2212 **Assessment evidence**

2213 1. List of methods of accessing memory and types of access control, output of tests
 2214

2215 [\[AC-CCON\]](#) Assessment criteria: Prevent creation of more than one user account

2216 **Assessment reference**

2217 Mitigation [MI-CCON](#).

2218 **Assessment objective**

2219 Prevent unauthorized access of memory

2220 **Assessment preparation**

2221 1. List all user accounts and verify there is exactly one

2222 **Assessment activities**

2223 1. Attempt to create a second user account, then list user accounts again

2224 **Assessment verdict**

2225 The verdict fail is assigned if any of the following conditions apply:

2226 1. Creation of second user account succeeds or list of user accounts is not identical before and after test

2227 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

2228 1. Creation of second user account fails and list of user accounts shows one account and is identical before and
 2229 after test

2230 **Assessment evidence**

2231 1. List of user accounts before and after test, output of test
 2232

2233 [\[AC-UCON\]](#) Assessment criteria: Prevent concurrent user account usage

2234 **Assessment reference**

2235 Mitigation [MI-UCON](#).

2236 **Assessment objective**

2237 Prevent unauthorized access of memory

2238 **Assessment preparation**

2239 1. Create two accounts, log in to one account, list all logged in user accounts and verify there is exactly one, list
 2240 all methods of logging in to a user account

2241 **Assessment activities**

2242 1. For each method of logging in to a user account, attempt to login as a second user account, then list logged in
 2243 user accounts again

2244 **Assessment verdict**

- 2245 The verdict fail is assigned if any of the following conditions apply:
 2246 1. Login of second user account succeeds, or list of user accounts logged in is not identical before and after test
- 2247 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
 2248 1. Login of second user account fails or is not possible, and list of user accounts logged in shows one account and
 2249 is identical before and after test
- 2250 **Assessment evidence**
 2251 1. List of logged in user accounts before and after test, output of each test or evidence proving that logging in as a
 2252 second user is impossible
 2253
- 2254 [\[AC-PMSC\]](#) Assessment criteria: Prevent memory leaks through microarchitectural side channels in provided
 2255 executables
- 2256 **Assessment reference**
 2257 Mitigation [MI-PMSC](#).
- 2258 **Assessment objective**
 2259 Prevent unauthorized reads of memory
- 2260 **Assessment preparation**
 2261 1. List known MASC leaks on supported platform
- 2262 **Assessment activities**
 2263 1. For each type of MASC leak, run a test using the best known techniques to exploit the MASC on a system-
 2264 provided executable
- 2265 **Assessment verdict**
 2266 The verdict fail is assigned if any of the following conditions apply:
 2267 1. Any test extracts data that it does not have authorization to read
 2268 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
 2269 1. All tests fail to extract data that they do not have authorization to read
- 2270 **Assessment evidence**
 2271 1. Output of each test
 2272
- 2273 [\[AC-RRMD\]](#) Assessment criteria: Document residual risk of microarchitectural side channel data leaks
- 2274 **Assessment reference**
 2275 Mitigation [MI-RRMD](#).
- 2276 **Assessment objective**
 2277 Prevent unauthorized reads of memory
- 2278 **Assessment activities**
 2279 1. Read documentation provided with the product
- 2280 **Assessment verdict**
 2281 The verdict fail is assigned if any of the following conditions apply:
 2282 1. Documentation does not describe the risks, or does not describe the configuration steps and operational
 2283 practices for mitigating them
 2284 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
 2285 1. Documentation describes the risks and the configuration steps and operational practices for mitigating them

2286 **Assessment evidence**

- 2287 1. Documentation provided with the product
-
- 2288

2289 **7.5 TR-MSAF: Mitigate memory safety errors**2290 [\[AC-MSAF-1\]](#) Assessment criteria: Stack exhaustion detection2291 **Assessment reference**2292 Mitigation [MI-MSAF-1](#).2293 **Assessment objective**

2294 Prevent thread from writing to memory immediately beyond the end of the stack

2295 **Assessment activities**

- 2296 1. For each execution context (e.g. kernel and userspace on products with privilege separation), write to memory
-
- 2297 beyond the end of the stack

2298 **Assessment verdict**

2299 The verdict fail is assigned if any of the following conditions apply:

- 2300 1. Any involved thread reads or writes the target data without taking a segmentation fault, without error handling
-
- 2301 code being executed, and without being terminated

2302 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2303 1. Each involved thread fails to read or write the target data and takes a segmentation fault, has error handling
-
- 2304 code executed, or is terminated in all tests

2305 **Assessment evidence**

- 2306 1. Error messages, log messages, or evidence that the product reboots or halts

2307 NOTE: Guidance: Two methods of exhausting stack memory include allocating a very large object on the stack,
2308 and performing an unbounded recursive function call.

2309

2310 [\[AC-MSAF-2\]](#) Assessment criteria: Stack linear buffer overflow detection2311 **Assessment reference**2312 Mitigation [MI-MSAF-2](#).2313 **Assessment objective**

2314 Prevent thread from writing to memory immediately beyond the end of the stack

2315 **Assessment activities**

- 2316 1. For each execution context (e.g. kernel and userspace on products with privilege separation), write beyond the
-
- 2317 end of the stack frame

2318 **Assessment verdict**

2319 The verdict fail is assigned if any of the following conditions apply:

- 2320 1. Any involved thread reads or writes the target data without taking a segmentation fault, without error handling
-
- 2321 code being executed, and without being terminated

2322 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2323 1. Each involved thread fails to read or write the target data and takes a segmentation fault, has error handling
-
- 2324 code executed, or is terminated in all tests

2325 **Assessment evidence**

- 2326 1. Error messages, log messages, or evidence that the product reboots or halts
-
- 2327

- 2328 [\[AC-MSAF-3\]](#) Assessment criteria: Array bounds checking
- 2329 **Assessment reference**
- 2330 Mitigation [MI-MSAF-3](#).
- 2331 **Assessment objective**
- 2332 Prevent thread from writing beyond the end of a fixed-size array
- 2333 **Assessment activities**
- 2334 1. For each execution context (e.g. kernel and userspace on products with privilege separation), write beyond the
- 2335 end of a fixed-size array
- 2336 **Assessment verdict**
- 2337 The verdict fail is assigned if any of the following conditions apply:
- 2338 1. Any involved thread reads or writes the target data without taking a segmentation fault, without error handling
- 2339 code being executed, and without being terminated
- 2340 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
- 2341 1. Each involved thread fails to read or write the target data and takes a segmentation fault, has error handling
- 2342 code executed, or is terminated in all tests
- 2343 **Assessment evidence**
- 2344 1. Error messages, log messages, or evidence that the product reboots or halts
- 2345
- 2346 [\[AC-MSAF-4\]](#) Assessment criteria: Heap linear buffer overflow detection
- 2347 **Assessment reference**
- 2348 Mitigation [MI-MSAF-4](#).
- 2349 **Assessment objective**
- 2350 Prevent thread from writing beyond the end of heap memory
- 2351 **Assessment activities**
- 2352 1. For each execution context (e.g. kernel and userspace on products with privilege separation), for each type of
- 2353 heap memory, allocate a fixed size from each class of heap memory, write beyond it
- 2354 **Assessment verdict**
- 2355 The verdict fail is assigned if any of the following conditions apply:
- 2356 1. Any involved thread reads or writes the target data without taking a segmentation fault, without error handling
- 2357 code being executed, and without being terminated
- 2358 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
- 2359 1. Each involved thread fails to read or write the target data and takes a segmentation fault, has error handling
- 2360 code executed, or is terminated in all tests
- 2361 **Assessment evidence**
- 2362 1. Error messages, log messages, or evidence that the product reboots or halts
- 2363
- 2364 [\[AC-MSAF-5\]](#) Assessment criteria: Heap use-after-free access prevention
- 2365 **Assessment reference**
- 2366 Mitigation [MI-MSAF-5](#).
- 2367 **Assessment objective**
- 2368 Prevent thread from using memory that was allocated then freed

2369 **Assessment activities**

- 2370 1. For each execution context (e.g. kernel and userspace on products with privilege separation), allocate from
 2371 heap memory, free it, then try to read it, repeat but with a write

2372 **Assessment verdict**

2373 The verdict fail is assigned if any of the following conditions apply:

- 2374 1. Any involved thread reads or writes the target data without taking a segmentation fault, without error handling
 2375 code being executed, and without being terminated

2376 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2377 1. Each involved thread fails to read or write the target data and takes a segmentation fault, has error handling
 2378 code executed, or is terminated in all tests

2379 **Assessment evidence**

- 2380 1. Error messages, log messages, or evidence that the product reboots or halts
 2381

2382 [\[AC-MSAF-6\]](#) Assessment criteria: Heap free checking

2383 **Assessment reference**

2384 Mitigation [MI-MSAF-6](#).

2385 **Assessment objective**

2386 Prevent thread from freeing memory that is already free

2387 **Assessment activities**

- 2388 1. For each execution context (e.g. kernel and userspace on products with privilege separation), allocate from
 2389 heap memory, free it, then free again

2390 **Assessment verdict**

2391 The verdict fail is assigned if any of the following conditions apply:

- 2392 1. Any involved thread reads or writes the target data without taking a segmentation fault, without error handling
 2393 code being executed, and without being terminated

2394 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2395 1. Each involved thread fails to read or write the target data and takes a segmentation fault, has error handling
 2396 code executed, or is terminated in all tests

2397 **Assessment evidence**

- 2398 1. Error messages, log messages, or evidence that the product reboots or halts
 2399

2400 **7.6 TR-LMII: Limit incident impact**

2401 [\[AC-MZRO-1\]](#) Assessment criteria: Stack memory zeroing

2402 **Assessment reference**

2403 Mitigation [MI-MZRO-1](#).

2404 **Assessment objective**

2405 Prevent attacker from exploiting erroneous use of uninitialized stack memory

2406 **Assessment activities**

- 2407 1. For each of kernel and userspace, sequentially call 2 functions that allocate the same amount of memory, fill
 2408 the first with non-zero values and return, and during second function call, read the stack contents back

2409 **Assessment verdict**

- 2410 The verdict fail is assigned if any of the following conditions apply:
- 2411 1. Stack contents are not all zero on the second call and the thread is not terminated when trying to read the stack
- 2412 contents back.
- 2413 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
- 2414 1. Stack contents are all zero on the second call or the thread is terminated when trying to read the stack contents
- 2415 back.
- 2416 **Assessment evidence**
- 2417 1. Contents of stack before the first function return, contents of stack during the second function call.
- 2418
- 2419 [\[AC-MZRO-2\]](#) Assessment criteria: Heap memory zeroing
- 2420 **Assessment reference**
- 2421 Mitigation [MI-MZRO-2](#).
- 2422 **Assessment objective**
- 2423 Prevent attacker from exploiting erroneous use of uninitialized heap memory
- 2424 **Assessment activities**
- 2425 1. For each of kernel and userspace, allocate heap memory, fill with a non-zero value, free it, allocate it again in a
- 2426 deterministic way to get the same heap region, and read back the contents
- 2427 **Assessment verdict**
- 2428 The verdict fail is assigned if any of the following conditions apply:
- 2429 1. Memory contents are not all zero on second call.
- 2430 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
- 2431 1. Memory contents are all zero on second call.
- 2432 **Assessment evidence**
- 2433 1. Contents of allocated memory before the free, contents of allocated memory after second allocation.
- 2434
- 2435 [\[AC-MRWX-1\]](#) Assessment criteria: Prevent writes to executable and read-only data memory
- 2436 **Assessment reference**
- 2437 Mitigation [MI-MRWX-1](#).
- 2438 **Assessment objective**
- 2439 Prevent writes to executable and read-only memory mappings
- 2440 **Assessment activities**
- 2441 1. Write to executable and read-only memory mappings in kernel and userspace
- 2442 **Assessment verdict**
- 2443 The verdict fail is assigned if any of the following conditions apply:
- 2444 1. Any involved thread reads or writes the target data without taking a segmentation fault, without error handling
- 2445 code being executed, and without being terminated
- 2446 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
- 2447 1. Each involved thread fails to read or write the target data and takes a segmentation fault, has error handling
- 2448 code executed, or is terminated in all tests
- 2449 **Assessment evidence**
- 2450 1. Error messages, log messages, or evidence that the product reboots or halts
- 2451

- 2452 [\[AC-MRWX-2\]](#) Assessment criteria: Prevent execution of non-kernel code memory
- 2453 **Assessment reference**
- 2454 Mitigation [MI-MRWX-2](#).
- 2455 **Assessment objective**
- 2456 Mitigate exploits that use execution of arbitrary memory
- 2457 **Assessment activities**
- 2458 1. For each class of non-code memory in the kernel (e.g. stack, heap, read-only data), copy a trivial return-only
- 2459 function into the memory, and attempt to execute each one
- 2460 **Assessment verdict**
- 2461 The verdict fail is assigned if any of the following conditions apply:
- 2462 1. Any involved thread reads or writes the target data without taking a segmentation fault, without error handling
- 2463 code being executed, and without being terminated
- 2464 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
- 2465 1. Each involved thread fails to read or write the target data and takes a segmentation fault, has error handling
- 2466 code executed, or is terminated in all tests
- 2467 **Assessment evidence**
- 2468 1. Error messages, log messages, or evidence that the product reboots or halts
- 2469
- 2470 [\[AC-ASLR\]](#) Assessment criteria: Address space layout randomization
- 2471 **Assessment reference**
- 2472 Mitigation [MI-ASLR](#).
- 2473 **Assessment objective**
- 2474 Exploit mitigation
- 2475 **Assessment activities**
- 2476 1. For every executable, examine the object file to determine if ASLR is enabled. For one non-kernel executable
- 2477 (if any) and one kernel executable (if any), run the executable twice and read the base addresses of the text,
- 2478 stack, heap, and shared libraries where applicable.
- 2479 **Assessment verdict**
- 2480 The verdict fail is assigned if any of the following conditions apply:
- 2481 1. Any executable does not have ASLR enabled, or base addresses collected for executables do not differ
- 2482 between runs.
- 2483 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
- 2484 1. All executables have ASLR enabled, base addresses collected for executables differ between runs.
- 2485 **Assessment evidence**
- 2486 1. Output of scan for ASLR enabled, base addresses collected.
- 2487
- 2488 [\[AC-MRCO\]](#) Assessment criteria: Mitigate reference counter overflow
- 2489 **Assessment reference**
- 2490 Mitigation [MI-MRCO](#).
- 2491 **Assessment objective**
- 2492 Prevent exploitation of bugs in reference counting to overflow the counter to zero, causing a free and subsequent use-
- 2493 after-free accesses

2494 **Assessment activities**

- 2495 1. For each of kernel and userspace, set resource reference counter to 1 less than maximum representable value,
2496 increment it twice

2497 **Assessment verdict**

2498 The verdict fail is assigned if any of the following conditions apply:

- 2499 1. Reference counter overflows or resource is not permanently pinned.

2500 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2501 1. Reference counter does not overflow and resource is permanently pinned (no longer can be freed).

2502 **Assessment evidence**

- 2503 1. Test output showing reference counter values before and after the operation, allocation status of the resources.
2504

2505 [\[AC-NKAM\]](#) Assessment criteria: Prevent unintentional kernel access to userspace memory

2506 **Assessment reference**

2507 Mitigation [MI-NKAM](#).

2508 **Assessment objective**

2509 Mitigate exploits that use kernel privileges to access arbitrary userspace memory

2510 **Assessment activities**

- 2511 1. For each of read, write, and execute operations, use a kernel thread to attempt to use the operation on memory
2512 regions that are mapped to a different privilege level without going through dedicated memory access routines

2513 **Assessment verdict**

2514 The verdict fail is assigned if any of the following conditions apply:

- 2515 1. Any involved thread reads or writes the target data without taking a segmentation fault, without error handling
2516 code being executed, and without being terminated

2517 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2518 1. Each involved thread fails to read or write the target data and takes a segmentation fault, has error handling
2519 code executed, or is terminated in all tests

2520 **Assessment evidence**

- 2521 1. Error messages, log messages, or evidence that the product reboots or halts
2522 NOTE: Guidance: The most common privilege levels are kernel and userspace.

2523

2524 [\[AC-PULS\]](#) Assessment criteria: Prevent use of uninitialized linked data structures

2525 **Assessment reference**

2526 Mitigation [MI-PULS](#).

2527 **Assessment objective**

2528 Prevent linked list corruption

2529 **Assessment activities**

- 2530 1. For each of kernel and userspace, add or delete an item to an uninitialized list

2531 **Assessment verdict**

2532 The verdict fail is assigned if any of the following conditions apply:

- 2533 1. Any involved thread reads or writes the target data without taking a segmentation fault, without error handling
2534 code being executed, and without being terminated

2535 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
 2536 1. Each involved thread fails to read or write the target data and takes a segmentation fault, has error handling
 2537 code executed, or is terminated in all tests

2538 **Assessment evidence**

2539 1. Error messages, log messages, or evidence that the product reboots or halts
 2540

2541 [\[AC-CFIN\]](#) Assessment criteria: Control flow integrity

2542 **Assessment reference**

2543 Mitigation [MI-CFIN](#).

2544 **Assessment objective**

2545 Mitigate exploits by preventing overwrite of function and return pointers

2546 **Assessment activities**

2547 1. For each of kernel and userspace, save a function pointer to the heap, overwrite it with a different function,
 2548 make indirect call to the saved function pointer, then repeat but with a return address that was stored to the
 2549 stack

2550 **Assessment verdict**

2551 The verdict fail is assigned if any of the following conditions apply:

2552 1. Any involved thread reads or writes the target data without taking a segmentation fault, without error handling
 2553 code being executed, and without being terminated

2554 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

2555 1. Each involved thread fails to read or write the target data and takes a segmentation fault, has error handling
 2556 code executed, or is terminated in all tests

2557 **Assessment evidence**

2558 1. Error messages, log messages, or evidence that the product reboots or halts

2559 NOTE: Guidance: This mitigation can be implemented via software (e.g. ASan) or hardware (e.g. Pointer
 2560 Authentication), or validating transitions of expected control flow graph (e.g. KCFI, Shadow Stack).

2561

2562 [\[AC-MPMT\]](#) Assessment criteria: Memory protection using memory tagging

2563 **Assessment reference**

2564 Mitigation [MI-MPMT](#).

2565 **Assessment objective**

2566 Mitigate exploits by preventing memory errors

2567 **Assessment activities**

2568 1. For each of kernel and userspace, allocate 2 adjacent memory regions with separate tags. Attempt to read and
 2569 write memory with a positive offset into trailing region from leading region's tagged pointer. Attempt to read
 2570 and write with negative offset into leading region using trailing region's tagged pointer. Free a region and read
 2571 and write to the region using the original tagged pointer.

2572 **Assessment verdict**

2573 The verdict fail is assigned if any of the following conditions apply:

2574 1. Any involved thread reads or writes the target data without taking a segmentation fault, without error handling
 2575 code being executed, and without being terminated

2576 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

2577 1. Each involved thread fails to read or write the target data and takes a segmentation fault, has error handling
 2578 code executed, or is terminated in all tests

2579 **Assessment evidence**

2580 1. Error messages, log messages, or evidence that the product reboots or halts

2581

2582 [\[AC-MPUI\]](#) Assessment criteria: MPU-based task isolation2583 **Assessment reference**2584 Mitigation [MI-MPUI](#).2585 **Assessment objective**

2586 Prevent memory corruption in one task from propagating to other tasks

2587 **Assessment activities**2588 1. From a test task, attempt to read and write memory regions allocated to a different task, including its stack and
2589 any private data regions. Repeat for at least two distinct task pairs.2590 **Assessment verdict**

2591 The verdict fail is assigned if any of the following conditions apply:

2592 1. Any access attempt succeeds without a fault, or the target task's memory is corrupted.

2593 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

2594 1. Each access attempt results in a memory protection fault and the accessing task is terminated or restarted
2595 without corrupting the target task's memory.2596 **Assessment evidence**

2597 1. Fault handler logs, memory contents of target task before and after the access attempts.

2598

2599 [\[AC-STKG\]](#) Assessment criteria: Stack overflow detection and containment2600 **Assessment reference**2601 Mitigation [MI-STKG](#).2602 **Assessment objective**

2603 Prevent stack overflow from corrupting adjacent memory

2604 **Assessment activities**2605 1. Run a task that recursively consumes stack memory beyond its allocated stack region. Examine whether the
2606 system detects the overflow and whether memory adjacent to the task's stack is corrupted.2607 **Assessment verdict**

2608 The verdict fail is assigned if any of the following conditions apply:

2609 1. The system does not detect the stack overflow, or memory adjacent to the task's stack is corrupted.

2610 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

2611 1. The system detects the stack overflow and memory adjacent to the task's stack is not corrupted.

2612 **Assessment evidence**2613 1. Fault handler logs or canary check results, memory dump of the region adjacent to the task's stack before and
2614 after the test.

2615

2616 **7.7 TR-MINI: Minimize impact on other devices and services**2617 [\[AC-RRIS\]](#) Assessment criteria: Document residual risk to other devices and services2618 **Assessment reference**2619 Mitigation [MI-RRIS](#).

2620 **Assessment objective**

2621 Minimize impact on other devices and services

2622 **Assessment activities**

2623 1. Examine the documentation

2624 **Assessment verdict**

2625 The verdict fail is assigned if any of the following conditions apply:

2626 1. Residual risk is not documented, or the documentation does not state the actions the user or the operational
2627 environment can take.

2628 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

2629 1. Residual risk is documented in plain language including the actions the user or the operational environment
2630 can take to mitigate it.

2631 **Assessment evidence**

2632 1. Documentation, analysis of documentation.
2633

2634 [\[AC-MNET\]](#) Assessment criteria: Minimize negative impact of network transmission

2635 **Assessment reference**

2636 Mitigation [MI-MNET](#).

2637 **Assessment objective**

2638 Minimise negative impact on others

2639 **Assessment preparation**

2640 1. List all sources of transmitted network data on the product

2641 **Assessment activities**

2642 1. For each method of sending network data, examine the documentation of the ways it can interfere with other
2643 products or services, and what methods the product uses to minimise that interference

2644 **Assessment verdict**

2645 The verdict fail is assigned if any of the following conditions apply:

2646 1. Any method of sending network data is not documented with ways it can interface and methods used to
2647 minimise.

2648 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

2649 1. Every method of sending network data is documented with ways it can interface and methods used to
2650 minimise.

2651 **Assessment evidence**

2652 1. All configuration files for network services, documentation of network services and their impact and methods
2653 to minimise it, internal lists of listening ports, results of an external port scan.
2654

2655 [\[AC-MAMP\]](#) Assessment criteria: Minimize negative impact of network traffic amplification

2656 **Assessment reference**

2657 Mitigation [MI-MAMP](#).

2658 **Assessment objective**

2659 Minimise negative impact on others

2660 **Assessment preparation**

- 2661 1. List all network services that return responses larger than the received packet without authorization of the
2662 source

2663 **Assessment activities**

- 2664 1. For each network service, examine the documentation of the steps taken to limit access, rate-limit, or otherwise
2665 mitigate the use of the service in traffic amplification attacks
2666 2. For each network service identified in the preparation step, send a minimal unauthenticated request and
2667 measure the size of the response. Calculate the amplification factor (response size divided by request size).

2668 **Assessment verdict**

2669 The verdict fail is assigned if any of the following conditions apply:

- 2670 1. Any method of sending network data is not documented with how its impact on others has been mitigated.
2671 2. Any network service responds to unauthenticated requests with an amplification factor exceeding the
2672 manufacturer's documented limit and no rate-limiting or access control is in place.

2673 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2674 1. Every method of sending network data is documented with how its impact on others has been mitigated.
2675 2. Every network service either requires authentication before responding, or has an amplification factor that does
2676 not exceed the manufacturer's documented limit, or has rate-limiting or access controls in place that prevent
2677 sustained amplification.

2678 **Assessment evidence**

- 2679 1. All configuration files for network services, documentation of network services and their impact and methods
2680 to minimise it, internal lists of listening ports, results of an external port scan.
2681 2. Request and response packet captures, calculated amplification factors, rate-limiting configuration,
2682 authentication requirements per service.
2683

2684 **7.8 TR-SDEF: Secure by default configuration**

2685 [\[AC-ADEF\]](#) Assessment criteria: Authorization required by default to access security-relevant assets

2686 **Assessment reference**

2687 Mitigation [MI-ADEF](#).

2688 **Assessment objective**

2689 Find any unauthorized access to security relevant assets in default configuration

2690 **Assessment preparation**

- 2691 1. List all interfaces allowing access to security-relevant assets

2692 **Assessment activities**

- 2693 1. For each interface, attempt to access security-relevant assets without authentication and authorization and
2694 record whether access was allowed or not

2695 **Assessment verdict**

2696 The verdict fail is assigned if any of the following conditions apply:

- 2697 1. Any interface allows access without authentication and authorization.

2698 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2699 1. Every interface does not allow access without authentication and authorization.

2700 **Assessment evidence**

- 2701 1. List of interfaces allowing access to security-relevant assets, record of activities used to attempt unauthorized
2702 access to security-relevant assets, log of results of attempts
2703

2704 [\[AC-PDDI-1\]](#) Assessment criteria: Document how to protect access to debug and management interfaces

- 2705 **Assessment reference**
 2706 Mitigation [MI-PDDI-1](#).
- 2707 **Assessment objective**
 2708 Secure by default
- 2709 **Assessment preparation**
 2710 1. Examine the documentation for how to protect or disable the debug/management interfaces of the product
- 2711 **Assessment activities**
 2712 1. Examine the product for undocumented debug/management interfaces, then follow the instructions in the
 2713 documentation to disable or protect each documented interface, then attempt to access the interface without
 2714 authorization
- 2715 **Assessment verdict**
 2716 The verdict fail is assigned if any of the following conditions apply:
 2717 1. Any debug/management interface is not documented or any interface is accessible without authorization after
 2718 following the documentation to protect or disable them.
 2719 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
 2720 1. All debug/management interfaces are documented as to how to disable or protect them, and no interfaces are
 2721 accessible without authorization after following the documentation to protect or disable them.
- 2722 **Assessment evidence**
 2723 1. Pictures of the product, list of discovered interfaces, comparison with documentation, notes as to which are
 2724 documented how to disable/protect, logs of protect/disable actions, logs of attempts to access interfaces after
 2725 protected or disabled
 2726
- 2727 [\[AC-PDDI-2\]](#) Assessment criteria: Protect or disable physical access to debug and management interfaces
- 2728 **Assessment reference**
 2729 Mitigation [MI-PDDI-2](#).
- 2730 **Assessment objective**
 2731 Secure by default
- 2732 **Assessment preparation**
 2733 1. Examine the documentation of the network- and localhost-accessible interfaces of the product and follow the
 2734 instructions to mitigate the risk of any necessary unprotected or enabled interfaces
- 2735 **Assessment activities**
 2736 1. As an unprivileged process running on the system, attempt to access the system's local debug and management
 2737 interfaces and make unauthorized changes. Additionally, scan accessible memory and inter-process-
 2738 communication mechanisms for undocumented debug and management interfaces.
- 2739 **Assessment verdict**
 2740 The verdict fail is assigned if any of the following conditions apply:
 2741 1. Any undocumented interface is found or any interface can be accessed without authorization and is not
 2742 documented as necessary or the instructions to the user do not document the procedure, the residual risk, or the
 2743 permitted user roles.
 2744 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
 2745 1. No undocumented interfaces are found and no interfaces can be accessed without authorization other than
 2746 those documented as necessary and the instructions to the user document the procedure, the residual risk, and
 2747 the permitted user roles.
- 2748 **Assessment evidence**

- 2749 1. List of interfaces, log of attempts to access
2750
- 2751 [\[AC-PDDI-3\]](#) Assessment criteria: Protect or disable local software access to debug and management interfaces
- 2752 **Assessment reference**
2753 Mitigation [MI-PDDI-3](#).
- 2754 **Assessment objective**
2755 Secure by default
- 2756 **Assessment preparation**
2757 1. Examine the documentation of the network- and localhost-accessible interfaces of the product and follow the
2758 instructions to mitigate the risk of any necessary unprotected or enabled interfaces
- 2759 **Assessment activities**
2760 1. As an unprivileged process running on the system, attempt to access the system's local debug and management
2761 interfaces and make unauthorized changes. Additionally, scan accessible memory and inter-process-
2762 communication mechanisms for undocumented debug and management interfaces.
- 2763 **Assessment verdict**
2764 The verdict fail is assigned if any of the following conditions apply:
2765 1. Any undocumented interface is found or any interface can be accessed without authorization and is not
2766 documented as necessary or the instructions to the user do not document the procedure, the residual risk, or the
2767 permitted user roles.
- 2768 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
2769 1. No undocumented interfaces are found and no interfaces can be accessed without authorization other than
2770 those documented as necessary and the instructions to the user document the procedure, the residual risk, and
2771 the permitted user roles.
- 2772 **Assessment evidence**
2773 1. List of interfaces, log of attempts to access
2774
- 2775 [\[AC-PDDI-4\]](#) Assessment criteria: Protect or disable network access to debug or management interfaces
- 2776 **Assessment reference**
2777 Mitigation [MI-PDDI-4](#).
- 2778 **Assessment objective**
2779 Secure by default
- 2780 **Assessment preparation**
2781 1. Examine the documentation of the network accessible interfaces of the product and follow the instructions to
2782 mitigate the risk of any necessary unprotected or enabled interfaces
- 2783 **Assessment activities**
2784 1. Using a network scanner, scan the product for both documented and undocumented debug or remote
2785 management interfaces and determine whether they are enabled or protected
- 2786 **Assessment verdict**
2787 The verdict fail is assigned if any of the following conditions apply:
2788 1. Any undocumented interface is found or any interface can be accessed without authorization and is not
2789 documented as necessary or the instructions to the user do not document the procedure, the residual risk, or the
2790 permitted user roles.
- 2791 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2792 1. No undocumented interfaces are found and no interfaces can be accessed without authorization other than
 2793 those documented as necessary and the instructions to the user document the procedure, the residual risk, and
 2794 the permitted user roles.

2795 **Assessment evidence**

- 2796 1. List of interfaces, log of attempts to access
 2797

2798 7.9 TR-SCUD: Secure updates

2799 [\[AC-KEVD\]](#) Assessment criteria: Documentation for secure update before or during first use

2800 **Assessment reference**

2801 Mitigation [MI-KEVD](#).

2802 **Assessment objective**

2803 Verify that the product documents a secure update mechanism for first use

2804 **Assessment preparation**

- 2805 1. Examine public or private vulnerability information sources and select a recently disclosed known exploitable
 2806 vulnerability, prioritising by severity, known exploitation in the wild, and impact on the product

2807 **Assessment activities**

- 2808 1. On a new product, carry out the initial secure update following the manufacturer's documentation, then scan
 2809 the product to verify that the selected known exploitable vulnerability has been addressed

2810 **Assessment verdict**

2811 The verdict fail is assigned if any of the following conditions apply:

- 2812 1. The secure update does not complete successfully, the selected known exploitable vulnerability is not
 2813 addressed, or the documentation does not include the required information

2814 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2815 1. The secure update completes successfully, the selected known exploitable vulnerability is addressed, and the
 2816 documentation includes the required information

2817 **Assessment evidence**

- 2818 1. Documentation of how to securely update the product, the report for the selected known exploitable
 2819 vulnerability, description of how to scan for the vulnerability, log of vulnerability scan results
 2820

2821 [\[AC-KEVA\]](#) Assessment criteria: Secure update before or during first use

2822 **Assessment reference**

2823 Mitigation [MI-KEVA](#).

2824 **Assessment objective**

2825 Verify that the product applies a secure update at first use

2826 **Assessment preparation**

- 2827 1. Examine public or private vulnerability information sources and select a recently disclosed known exploitable
 2828 vulnerability, prioritising by severity, known exploitation in the wild, and impact on the product

2829 **Assessment activities**

- 2830 1. Follow the instructions to install and use the product for the first time, verify that the secure update mechanism
 2831 activates before or during first use, then scan the product to verify that the selected known exploitable
 2832 vulnerability has been addressed

2833 **Assessment verdict**

2834 The verdict fail is assigned if any of the following conditions apply:

- 2835 1. The secure update mechanism does not activate before or during first use, the selected known exploitable
2836 vulnerability is not addressed, or the documentation does not include the required information

2837 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2838 1. The secure update mechanism activates before or during first use, the selected known exploitable vulnerability
2839 is addressed, and the documentation includes the required information

2840 **Assessment evidence**

- 2841 1. Documentation of the secure update mechanism, the report for the selected known exploitable vulnerability,
2842 description of how to scan for the vulnerability, log of vulnerability scan results
2843

2844 [\[AC-SCHL\]](#) Assessment criteria: Low security updates provided by operational environment

2845 **Assessment reference**

2846 Mitigation [MI-SCHL](#).

2847 **Assessment objective**

2848 Secure updates

2849 **Assessment activities**

- 2850 1. Assess the documentation provided with the product

2851 **Assessment verdict**

2852 The verdict fail is assigned if any of the following conditions apply:

- 2853 1. Documentation does not describe requirements for the secure updates provided by the operational
2854 environment.

2855 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2856 1. Documentation describes requirements for the secure updates provided by the operational environment.

2857 **Assessment evidence**

- 2858 1. Documentation and analysis of completeness
2859

2860 [\[AC-SCHM\]](#) Assessment criteria: Medium security updates provided by operational environment

2861 **Assessment reference**

2862 Mitigation [MI-SCHM](#).

2863 **Assessment objective**

2864 Secure updates

2865 **Assessment activities**

- 2866 1. Assess the documentation provided with the product

2867 **Assessment verdict**

2868 The verdict fail is assigned if any of the following conditions apply:

- 2869 1. Documentation does not describe requirements for the secure updates provided by the operational
2870 environment.

2871 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2872 1. Documentation describes requirements for the secure updates provided by the operational environment.

2873 **Assessment evidence**

- 2874 1. Documentation and analysis of completeness
2875

2876 [\[AC-SCHH\]](#) Assessment criteria: High security updates provided by operational environment

2877 **Assessment reference**

2878 Mitigation [MI-SCHH](#).

2879 **Assessment objective**

2880 Secure updates

2881 **Assessment activities**

2882 1. Assess the documentation provided with the product

2883 **Assessment verdict**

2884 The verdict fail is assigned if any of the following conditions apply:

2885 1. Documentation does not describe requirements for the secure updates provided by the operational
2886 environment.

2887 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

2888 1. Documentation describes requirements for the secure updates provided by the operational environment.

2889 **Assessment evidence**

2890 1. Documentation and analysis of completeness

2891

2892 7.10 TR-AUTH: Authentication and access control

2893 [\[AC-RAUT\]](#) Assessment criteria: Authenticate the remote data processing solution at the RDPS boundary

2894 **Assessment reference**

2895 Mitigation [MI-RAUT](#).

2896 **Assessment objective**

2897 Authenticate the remote data processing solution at the RDPS boundary

2898 **Assessment preparation**

2899 1. Documentation describing the authentication mechanism used for communication with each remote data
2900 processing solution is available.

2901 2. The product is in operational state with remote data processing solution connectivity configured.

2902 **Assessment activities**

2903 1. Review the documentation to identify the authentication mechanism used by the product to authenticate the
2904 remote data processing solution before transmitting data or acting upon received interactions.

2905 2. Substitute the remote data processing solution with an endpoint that does not satisfy authentication. Observe
2906 whether the product transmits data to, or acts upon interactions from, the substituted endpoint.

2907 **Assessment verdict**

2908 The verdict fail is assigned if any of the following conditions apply:

2909 1. Documentation does not describe the authentication mechanism used by the product to authenticate the remote
2910 data processing solution.

2911 2. The product transmits data to, or acts upon interactions from, an endpoint that does not satisfy authentication.

2912 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

2913 1. Documentation describes the authentication mechanism used by the product to authenticate the remote data
2914 processing solution.

2915 2. The product does not transmit data to, or act upon interactions from, an endpoint that does not satisfy
2916 authentication.

2917 **Assessment evidence**

- 2918 1. Documentation describing the authentication mechanism used by the product.
 2919 2. Test results showing the product authenticates the remote data processing solution before transmitting data or
 2920 acting upon interactions.
 2921
- 2922 [\[AC-AUTH\]](#) Assessment criteria: Require authentication on interfaces providing access to the operating system
- 2923 **Assessment reference**
 2924 Mitigation [MI-AUTH](#).
- 2925 **Assessment objective**
 2926 Require authentication on interfaces providing access to the operating system.
- 2927 **Assessment preparation**
 2928 1. List all interfaces through which the operating system exposes access to operating-system resources or
 2929 functions, including login interfaces (such as PAM-based text and graphical logins, remote shell daemons,
 2930 console interfaces), programmatic interfaces requiring user or administrator context (such as privilege-
 2931 elevation utilities, management APIs, and administrative tooling), and remote management interfaces provided
 2932 by the operating system.
 2933 2. Documentation describing the authentication mechanism applied to each interface, the set of functions the
 2934 interface exposes, and any interfaces deliberately not requiring authentication together with the justification for
 2935 the exception.
- 2936 **Assessment activities**
 2937 1. Review the documentation to verify that every interface providing access to operating-system resources or
 2938 functions either requires user or administrator authentication or is documented as deliberately unauthenticated
 2939 with justification.
 2940 2. For each documented authenticated interface, attempt to access operating-system resources or functions
 2941 through that interface without presenting valid authentication. Verify that access is denied.
- 2942 **Assessment verdict**
 2943 The verdict fail is assigned if any of the following conditions apply:
 2944 1. Any interface providing access to operating-system resources or functions neither requires authentication nor is
 2945 documented as deliberately unauthenticated with justification.
 2946 2. Any documented authenticated interface grants access without valid authentication.
 2947 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
 2948 1. Every interface either requires authentication or is documented as deliberately unauthenticated with
 2949 justification.
 2950 2. Every documented authenticated interface denies access without valid authentication.
- 2951 **Assessment evidence**
 2952 1. Documentation listing every interface, its authentication mechanism, and any unauthenticated-interface
 2953 justifications.
 2954 2. Test results showing that each authenticated interface denies access without authentication.
 2955
- 2956 [\[AC-LCKT\]](#) Assessment criteria: Authentication failure protection
- 2957 **Assessment reference**
 2958 Mitigation [MI-LCKT](#).
- 2959 **Assessment objective**
 2960 Prevent brute-force attacks against operating-system authentication interfaces.
- 2961 **Assessment preparation**
 2962 1. Documentation describing, for each authentication interface, the progressive-delay behaviour, the configurable
 2963 failure-count threshold that triggers temporary lockout, and the lockout duration.

2964 **Assessment activities**

- 2965 1. Review the documentation to verify that every authentication interface is associated with documented
2966 progressive-delay behaviour and a configurable failure-count threshold for temporary lockout.
2967 2. For each authentication interface, perform authentication attempts with invalid credentials. Verify that the
2968 delay between successive attempts increases progressively, and that after the documented number of failed
2969 attempts the account or interface temporarily locks out further attempts.

2970 **Assessment verdict**

2971 The verdict fail is assigned if any of the following conditions apply:

- 2972 1. Any authentication interface lacks documented progressive-delay behaviour or a configurable failure-count
2973 threshold.
2974 2. Any authentication interface does not exhibit progressive delays or does not lock out after the documented
2975 threshold.

2976 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2977 1. Every authentication interface is associated with documented progressive-delay behaviour and a configurable
2978 failure-count threshold.
2979 2. Every authentication interface exhibits progressive delays between failed attempts and temporary lockout after
2980 the documented threshold.

2981 **Assessment evidence**

- 2982 1. Documentation listing, per authentication interface, the progressive-delay behaviour and the failure-count
2983 threshold.
2984 2. Test results showing progressive delays and temporary lockout behaviour per interface.
2985

2986 [\[AC-CRED\]](#) Assessment criteria: Protect stored critical security parameters and enforce credential entropy

2987 **Assessment reference**

2988 Mitigation [MI-CRED](#).

2989 **Assessment objective**

2990 Protect stored credentials and critical security parameters and enforce minimum credential entropy on accepted
2991 credentials.

2992 **Assessment preparation**

- 2993 1. List all categories of critical security parameters stored by the operating system, including credential hashes or
2994 equivalent verification material, cryptographic keys managed by kernel keyrings or operating-system key
2995 stores, certificate private keys, and trust anchors.
2996 2. Documentation describing the protection mechanism applied to each category of stored critical security
2997 parameter, conforming to TR-CRYP, and the minimum credential entropy requirements enforced by each
2998 authentication interface.

2999 **Assessment activities**

- 3000 1. Review the documentation to verify that every category of stored critical security parameter is associated with
3001 a documented protection mechanism conforming to TR-CRYP, and that every authentication interface is
3002 associated with a documented minimum credential entropy requirement.
3003 2. Inspect the storage representation of each category of critical security parameter on the operating system and
3004 verify that the documented protection mechanism is applied.
3005 3. For each authentication interface, attempt to configure a credential that does not meet the documented
3006 minimum entropy requirement. Verify that the operating system rejects the attempt.

3007 **Assessment verdict**

3008 The verdict fail is assigned if any of the following conditions apply:

- 3009 1. Any category of stored critical security parameter lacks a documented protection mechanism conforming to
3010 TR-CRYP, or any authentication interface lacks a documented minimum credential entropy requirement.
3011 2. The documented protection mechanism is not applied to any category of stored critical security parameter.

3012 3. Any authentication interface accepts a credential that does not meet the documented minimum entropy
3013 requirement.

3014 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3015 1. Every category of stored critical security parameter is associated with a documented protection mechanism
3016 conforming to TR-CRYP, and every authentication interface is associated with a documented minimum
3017 credential entropy requirement.
- 3018 2. The documented protection mechanism is applied to every category of stored critical security parameter.
- 3019 3. Every authentication interface rejects credentials that do not meet the documented minimum entropy
3020 requirement.

3021 **Assessment evidence**

- 3022 1. Documentation listing categories of stored critical security parameters with their protection mechanisms, and
3023 the minimum credential entropy requirements per authentication interface.
- 3024 2. Test results showing the storage representation of each category of critical security parameter and the
3025 protection mechanism applied.
- 3026 3. Test results showing rejection of low-entropy credentials per authentication interface.
3027

3028 [\[AC-ACCS\]](#) Assessment criteria: Access control enforcement on operating-system resources and functions

3029 **Assessment reference**

3030 Mitigation [MI-ACCS](#).

3031 **Assessment objective**

3032 Enforce access control on operating-system resources and functions.

3033 **Assessment preparation**

- 3034 1. Documentation describing the access control model used by the operating system, including the mechanism
3035 (such as discretionary access control through filesystem permissions, POSIX capabilities, mandatory access
3036 control frameworks, role-based access control, or compile-time fixed access rules), the protected resource
3037 categories, and the authorization attributes considered when granting access.

3038 **Assessment activities**

- 3039 1. Review the documentation to verify that the access control model is described, the protected resource
3040 categories are enumerated, and the authorization attributes are defined.
- 3041 2. For each protected resource category, attempt access from a subject that is authorized according to the
3042 documented model and verify the access succeeds. Attempt access from a subject that is not authorized
3043 according to the documented model and verify the access is denied.

3044 **Assessment verdict**

3045 The verdict fail is assigned if any of the following conditions apply:

- 3046 1. Documentation does not describe the access control model, the protected resource categories, or the
3047 authorization attributes.
- 3048 2. Any authorized subject is denied access or any unauthorized subject is permitted access for any protected
3049 resource category.

3050 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3051 1. Documentation describes the access control model, the protected resource categories, and the authorization
3052 attributes.
- 3053 2. Authorized subjects are permitted access and unauthorized subjects are denied access for every protected
3054 resource category.

3055 **Assessment evidence**

- 3056 1. Documentation describing the access control model, protected resource categories, and authorization attributes.
- 3057 2. Test results showing access outcomes for authorized and unauthorized subjects per protected resource
3058 category.
3059

3060 [\[AC-PRIV\]](#) Assessment criteria: Privilege separation and restriction

3061 **Assessment reference**

3062 Mitigation [MI-PRIV](#).

3063 **Assessment objective**

3064 Enforce privilege separation and restrict subjects to their assigned privilege level on operating systems supporting
3065 multiple privilege levels.

3066 **Assessment preparation**

3067 1. Documentation describing the privilege-level model of the operating system, including the distinct privilege
3068 levels (such as kernel and user mode, POSIX effective user identifiers, POSIX capabilities sets, or ring-based
3069 privilege hierarchies), the operations permitted at each privilege level, and the transitions between privilege
3070 levels.

3071 **Assessment activities**

3072 1. Review the documentation to verify that the distinct privilege levels, the operations permitted at each privilege
3073 level, and the transitions between privilege levels are described.
3074 2. For each privilege level, attempt to perform operations not permitted at that privilege level from a subject
3075 executing at that privilege level. Verify that the operating system denies the operation.

3076 **Assessment verdict**

3077 The verdict fail is assigned if any of the following conditions apply:

3078 1. Documentation does not describe the distinct privilege levels, the operations permitted at each privilege level,
3079 or the transitions between privilege levels.
3080 2. Any subject can perform an operation not permitted at its assigned privilege level.

3081 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

3082 1. Documentation describes the distinct privilege levels, the operations permitted at each privilege level, and the
3083 transitions between privilege levels.
3084 2. Every subject is restricted to the operations permitted at its assigned privilege level.

3085 **Assessment evidence**

3086 1. Documentation describing the privilege-level model.
3087 2. Test results showing denial of unauthorized operations per privilege level.
3088

3089 [\[AC-SESS\]](#) Assessment criteria: Session lifecycle controls

3090 **Assessment reference**

3091 Mitigation [MI-SESS](#).

3092 **Assessment objective**

3093 Enforce session lifecycle controls on authenticated sessions.

3094 **Assessment preparation**

3095 1. Documentation describing the session model of the operating system, including the default and configurable
3096 idle-timeout periods, the events that trigger session invalidation, and the authorization requirements for
3097 privilege escalation within an active session.

3098 **Assessment activities**

3099 1. Review the documentation to verify that the session model, the default and configurable idle-timeout periods,
3100 the session-invalidation triggers, and the privilege-escalation authorization requirements are described.
3101 2. Establish an authenticated session, leave the session idle for longer than the documented idle-timeout period,
3102 and verify that the session is invalidated.
3103 3. Establish an authenticated session, perform the documented session-invalidation triggers (logout or
3104 termination, authentication credential change), and verify that the session is invalidated immediately in each

3105 case. In an active session, attempt to elevate privileges without providing the documented authorization, and
3106 verify that the elevation is denied.

3107 **Assessment verdict**

3108 The verdict fail is assigned if any of the following conditions apply:

- 3109 1. Documentation does not describe the session model, the idle-timeout periods, the session-invalidation triggers,
3110 or the privilege-escalation authorization requirements.
- 3111 2. The session is not invalidated after the documented idle-timeout period.
- 3112 3. The session is not invalidated on any documented invalidation trigger, or privilege escalation within an active
3113 session succeeds without the documented authorization.

3114 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3115 1. Documentation describes the session model, the idle-timeout periods, the session-invalidation triggers, and the
3116 privilege-escalation authorization requirements.
- 3117 2. The session is invalidated after the documented idle-timeout period.
- 3118 3. The session is invalidated immediately on every documented invalidation trigger, and privilege escalation
3119 within an active session is denied without the documented authorization.

3120 **Assessment evidence**

- 3121 1. Documentation describing the session lifecycle.
- 3122 2. Test results showing session invalidation after the idle-timeout period.
- 3123 3. Test results showing immediate session invalidation on each trigger and denial of unauthorized privilege
3124 escalation.
- 3125

3126 7.11 TR-CRYP: Encryption

3127 [\[AC-CRYP\]](#) Assessment criteria: State of the art cryptography

3128 **Assessment reference**

3129 Mitigation [MI-CRYP](#).

3130 **Assessment objective**

3131 Confirm that the operating system requires state of the art cryptography for all cryptographic functions it provides or
3132 uses, and that no deprecated or weak cryptography is enabled.

3133 **Assessment preparation**

- 3134 1. Documentation describing the cryptographic configuration of the operating system is available, listing the
3135 cryptographic functions provided by the operating system to applications, the cryptographic functions used by
3136 the operating system itself, the system-wide cryptographic policy configuration, the algorithms used for kernel
3137 module signature verification and boot integrity, and the system random number generation mechanism.

3138 **Assessment activities**

- 3139 1. Review the documentation to identify the cryptographic configuration of the operating system.
- 3140 2. Inspect the operating system in its factory default state to verify that the active cryptographic configuration
3141 matches the documented configuration and is state of the art.
- 3142 3. Inspect the operating system in its operational state to verify that the active cryptographic configuration
3143 matches the documented configuration and is state of the art.
- 3144 4. Verify that where cryptographic negotiation is supported by the operating system, the default negotiation order
3145 does not prefer deprecated cryptography over recognized cryptography, and that where only fixed
3146 configuration is used, no cryptographic negotiation occurs.

3147 **Assessment verdict**

3148 The verdict fail is assigned if any of the following conditions apply:

- 3149 1. Documentation does not describe the cryptographic configuration of the operating system.
- 3150 2. The operating system does not use state of the art cryptography in its factory default state.
- 3151 3. The operating system does not use state of the art cryptography in its operational state.

- 3152 4. The operating system does not prioritize recognized cryptography over deprecated cryptography in the default
 3153 negotiation order where negotiation is supported.
 3154 5. The operating system performs cryptographic negotiation where only fixed configuration is used.

3155 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3156 1. Documentation describes the cryptographic configuration of the operating system.
 3157 2. The operating system uses state of the art cryptography in its factory default state.
 3158 3. The operating system uses state of the art cryptography in its operational state.
 3159 4. The operating system prioritizes recognized cryptography over deprecated cryptography in the default
 3160 negotiation order where negotiation is supported.
 3161 5. The operating system does not perform cryptographic negotiation where only fixed configuration is used.

3162 **Assessment evidence**

- 3163 1. Documentation describing the cryptographic configuration of the operating system.
 3164 2. Test results showing the cryptographic configuration is state of the art in the factory default state.
 3165 3. Test results showing the cryptographic configuration is state of the art in the operational state.
 3166 4. Test results showing the default negotiation order does not prefer deprecated cryptography over recognized
 3167 cryptography where negotiation is supported.
 3168 5. Test results showing no cryptographic negotiation occurs where only fixed configuration is used.
 3169

3170 7.12 TR-CDST: Confidentiality of data stored on the product

3171 [\[AC-CDST\]](#) Assessment criteria: Protect confidentiality of data stored on the product

3172 **Assessment reference**

3173 Mitigation [MI-CDST](#).

3174 **Assessment objective**

3175 Confidentiality of data

3176 **Assessment preparation**

- 3177 1. List all types of data that may be stored on the product that should not be readable without authorization, the
 3178 confidentiality mechanism documented by the manufacturer for each type, all methods of accessing that data
 3179 available to an attacker based on the risk assessment, and the authorization methods documented by the
 3180 manufacturer for each access method

3181 **Assessment activities**

- 3182 1. For each type of data and each access mechanism, determine the method of ensuring confidentiality used, and
 3183 attempt to read the data without authorization

3184 **Assessment verdict**

3185 The verdict fail is assigned if any of the following conditions apply:

- 3186 1. Any method of ensuring confidentiality does not match the type of the data stored, or any attempt to read
 3187 confidential data without authorization succeeds.

3188 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3189 1. All methods of ensuring confidentiality match the type of the data stored, and all the attempts to read
 3190 confidential data without authorization fail.

3191 **Assessment evidence**

- 3192 1. Logs of determination of type of data and method of confidentiality and attempts to read confidential data
 3193 without authorization

3194 NOTE: Guidance: Data may be protected by the environment, permissions, encryption, salting and hashing,
 3195 offline storage, or hardware-backed secrets. Where encryption is used, cryptographic algorithms shall
 3196 conform to TR-CRYP.

3197

3198 [\[AC-FCST\]](#) Assessment criteria: Formal proof of enforcement of confidentiality of data stored on the product

3199 **Assessment reference**

3200 Mitigation [MI-FCST](#).

3201 **Assessment objective**

3202 Confidentiality of data

3203 **Assessment activities**

3204 1. Review the tool selection and configuration criteria documented by the manufacturer, the source code for the
3205 product, the formal definition of confidentiality, and the formal argument that it applies to a formalization of
3206 the product's source code

3207 **Assessment verdict**

3208 The verdict fail is assigned if any of the following conditions apply:

3209 1. The tool selection or configuration criteria are not documented, or the formal definition of confidentiality does
3210 not demonstrate the enforcement of confidentiality of data stored on the product, or the formal verification tool
3211 does not successfully output a proof.

3212 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

3213 1. The tool selection and configuration criteria are documented, the formal definition of confidentiality
3214 demonstrates the enforcement of confidentiality of data stored on the product, the formal verification tool
3215 successfully outputs a proof that the confidentiality statement is satisfied by the product.

3216 **Assessment evidence**

3217 1. The documentation documenting the tool selection and configuration criteria, how the tool is run, the source
3218 code for the product, the formal definition of the confidentiality, and the formal argument that it applies to a
3219 formalization of the product's source code
3220

3221 [\[AC-ENST\]](#) Assessment criteria: Cryptographic encryption of stored data

3222 **Assessment reference**

3223 Mitigation [MI-ENST](#).

3224 **Assessment objective**

3225 Protect the confidentiality of stored confidentiality-sensitive data using a cryptographic encryption mechanism.

3226 **Assessment preparation**

3227 1. List all categories of data stored by the operating system for which unauthorized access would lead to a
3228 security incident, including data stored in operating-system-managed storage such as filesystems and block
3229 devices, credential and cryptographic-key stores, certificate stores, kernel keyrings, swap space and hibernation
3230 files, crash dumps and core files, persistent log files containing sensitive events, and configuration stores
3231 holding critical security parameters.
3232 2. Documentation describing the cryptographic encryption mechanism applied to each category of stored
3233 confidentiality-sensitive data is available, including the algorithm used, the keying material or key-derivation
3234 mechanism, and the hardware-backed or software-backed key-storage mechanism used to protect the
3235 encryption keys.

3236 **Assessment activities**

3237 1. Review the documentation to verify that every category of confidentiality-sensitive stored data is associated
3238 with a documented cryptographic encryption mechanism conforming to TR-CRYP.
3239 2. Inspect the operating system in its operational state and examine the raw storage representation of each
3240 category of confidentiality-sensitive data. Verify that the documented cryptographic encryption mechanism is
3241 applied and that the algorithm in use matches the documentation and conforms to TR-CRYP.
3242 3. For each category of confidentiality-sensitive stored data, attempt to recover the stored content from the raw
3243 storage representation without access to the keying material. Verify that the content cannot be recovered.

3244 **Assessment verdict**

3245 The verdict fail is assigned if any of the following conditions apply:

- 3246 1. Documentation does not associate every category of confidentiality-sensitive stored data with a cryptographic
3247 encryption mechanism, or any documented mechanism does not conform to TR-CRYP.
- 3248 2. The cryptographic encryption mechanism is not applied to any category of confidentiality-sensitive stored
3249 data, or the algorithm in use does not conform to TR-CRYP.
- 3250 3. The stored content can be recovered from the raw storage representation without access to the keying material.

3251 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3252 1. Documentation associates every category of confidentiality-sensitive stored data with a cryptographic
3253 encryption mechanism conforming to TR-CRYP.
- 3254 2. The cryptographic encryption mechanism is applied to every category of confidentiality-sensitive stored data
3255 and the algorithm in use conforms to TR-CRYP.
- 3256 3. The stored content cannot be recovered from the raw storage representation without access to the keying
3257 material.

3258 **Assessment evidence**

- 3259 1. Documentation listing every category of confidentiality-sensitive stored data and the cryptographic encryption
3260 mechanism applied to each.
- 3261 2. Test results showing the raw storage representation of each category of stored data and the cryptographic
3262 encryption mechanism applied to it.
- 3263 3. Test results showing that stored content cannot be recovered from the raw storage representation without
3264 access to the keying material.
- 3265

3266 **7.13 TR-CDTX: Confidentiality of data transmitted by product**3267 [\[AC-CDTX\]](#) Assessment criteria: Protect confidentiality of data transmitted by product3268 **Assessment reference**3269 Mitigation [MI-CDTX](#).3270 **Assessment objective**

3271 Confidentiality of data

3272 **Assessment preparation**

- 3273 1. List all types of data that may be transmitted on the product that should not be readable without authorization,
3274 the confidentiality mechanism documented by the manufacturer for each type, all methods of accessing that
3275 data available to an attacker based on the risk assessment, and the authorization methods documented by the
3276 manufacturer for each access method

3277 **Assessment activities**

- 3278 1. For each type of data and each access mechanism, determine the method of ensuring confidentiality used, and
3279 attempt to read the data without authorization

3280 **Assessment verdict**

3281 The verdict fail is assigned if any of the following conditions apply:

- 3282 1. Any method of ensuring confidentiality does not match the type of the data transmitted, or any attempt to read
3283 confidential data without authorization succeeds.

3284 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3285 1. All methods of ensuring confidentiality match the type of the data transmitted, and all the attempts to read
3286 confidential data without authorization fail.

3287 **Assessment evidence**

- 3288 1. Logs of determination of type of data and method of confidentiality and attempts to read confidential data
3289 without authorization

3290 NOTE: Guidance: Data transmitted may be protected by the environment or by encryption. Where encryption is
 3291 used, cryptographic algorithms shall conform to TR-CRYP.

3292

3293 [\[AC-RRDC\]](#) Assessment criteria: Document residual risk to confidentiality of data transmitted

3294 **Assessment reference**

3295 Mitigation [MI-RRDC](#).

3296 **Assessment objective**

3297 Protect data confidentiality

3298 **Assessment activities**

3299 1. Examine the documentation

3300 **Assessment verdict**

3301 The verdict fail is assigned if any of the following conditions apply:

3302 1. Transfer of risk is not documented, or the documentation does not state the residual risks or the user
 3303 mitigations.

3304 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

3305 1. Transfer of risk is documented in plain language including the residual risks accepted by the user and the
 3306 actions the user can take to mitigate them.

3307 **Assessment evidence**

3308 1. Documentation, analysis of documentation

3309

3310 [\[AC-ENTX\]](#) Assessment criteria: Cryptographic encryption of transmitted data

3311 **Assessment reference**

3312 Mitigation [MI-ENTX](#).

3313 **Assessment objective**

3314 Protect the confidentiality of transmitted confidentiality-sensitive data using a cryptographic encryption mechanism.

3315 **Assessment preparation**

3316 1. List all categories of data transmitted by the operating system for which unauthorized disclosure would lead to
 3317 a security incident, including data transmitted through operating-system-provided network protocols (such as
 3318 TLS, SSH, IPsec, and VPN client or server implementations), remote administration interfaces, remote
 3319 filesystem and file sharing protocols, remote logging and audit streams, remote management or telemetry
 3320 channels, and channels exchanging credentials, cryptographic keys, or other critical security parameters.

3321 2. Documentation describing the cryptographic encryption mechanism applied to each category of transmitted
 3322 confidentiality-sensitive data is available, including the algorithm used, the keying material or session key
 3323 used, and the key establishment or negotiation mechanism.

3324 **Assessment activities**

3325 1. Review the documentation to verify that every category of confidentiality-sensitive transmitted data is
 3326 associated with a documented cryptographic encryption mechanism conforming to TR-CRYP.

3327 2. Inspect the operating system in its operational state while it transmits data in each documented category.
 3328 Capture the transmitted data on the network and verify that the documented cryptographic encryption
 3329 mechanism is applied and that the algorithm in use matches the documentation and conforms to TR-CRYP.

3330 3. For each category of confidentiality-sensitive transmitted data, attempt to recover the transmitted content from
 3331 a passive network capture without access to the keying material. Verify that the content cannot be recovered.

3332 **Assessment verdict**

3333 The verdict fail is assigned if any of the following conditions apply:

- 3334 1. Documentation does not associate every category of confidentiality-sensitive transmitted data with a
3335 cryptographic encryption mechanism, or any documented mechanism does not conform to TR-CRYP.
3336 2. The cryptographic encryption mechanism is not applied to any category of confidentiality-sensitive transmitted
3337 data, or the algorithm in use does not conform to TR-CRYP.
3338 3. The transmitted content can be recovered from the network capture without access to the keying material.

3339 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3340 1. Documentation associates every category of confidentiality-sensitive transmitted data with a cryptographic
3341 encryption mechanism conforming to TR-CRYP.
3342 2. The cryptographic encryption mechanism is applied to every category of confidentiality-sensitive transmitted
3343 data and the algorithm in use conforms to TR-CRYP.
3344 3. The transmitted content cannot be recovered from the network capture without access to the keying material.

3345 **Assessment evidence**

- 3346 1. Documentation listing every category of confidentiality-sensitive transmitted data and the cryptographic
3347 encryption mechanism applied to each.
3348 2. Test results from network traffic captures showing the cryptographic encryption mechanism applied to each
3349 category of confidentiality-sensitive transmitted data and the algorithm in use.
3350 3. Test results showing that transmitted content cannot be recovered from the network capture without access to
3351 the keying material.
3352

3353 7.14 TR-IDST: Integrity of data stored on the product

3354 [\[AC-IDST\]](#) Assessment criteria: Protect integrity of data stored on the product

3355 **Assessment reference**

3356 Mitigation [MI-IDST](#).

3357 **Assessment objective**

3358 Integrity of data

3359 **Assessment preparation**

- 3360 1. List all types of data that may be stored on the product that should not be modifiable without authorization, the
3361 integrity protection mechanism documented by the manufacturer for each type, all methods of modifying that
3362 data available to an attacker based on the risk assessment, and what the allowable authorization methods are
3363 for that modification method

3364 **Assessment activities**

- 3365 1. For each type of data and each access mechanism, determine the method of protecting integrity used, and
3366 attempt to modify the data without authorization

3367 **Assessment verdict**

3368 The verdict fail is assigned if any of the following conditions apply:

- 3369 1. Any method of ensuring integrity does not match the type of the data stored, or any attempt to modify
3370 protected data without authorization succeeds.

3371 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3372 1. All methods of ensuring integrity match the type of the data stored, and all the attempts to modify protected
3373 data without authorization fail.

3374 **Assessment evidence**

- 3375 1. Logs of determination of type of data and method of integrity and attempts to modify protected data without
3376 authorization

3377 NOTE: Guidance: Integrity may be protected by the environment, permissions, duplication, backups, checksums,
3378 or cryptographic integrity mechanisms. Where cryptographic integrity mechanisms are used,
3379 cryptographic algorithms shall conform to TR-CRYP.

3380

3381 [\[AC-DCST\]](#) Assessment criteria: Detect corruption of data stored3382 **Assessment reference**3383 Mitigation [MI-DCST](#).3384 **Assessment objective**

3385 Integrity of data

3386 **Assessment preparation**

3387 1. List all types of data that may be stored on the product whose corruption should be detected and the corruption
3388 detection mechanism documented by the manufacturer for each type

3389 **Assessment activities**

3390 1. For each type of data and method of detecting corruption, corrupt the data in a way that the method will detect

3391 **Assessment verdict**

3392 The verdict fail is assigned if any of the following conditions apply:

3393 1. Any method of detecting corruption does not match the type of the data stored, or any corruption of data is not
3394 detected.

3395 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

3396 1. All methods of detecting corruption match the type of the data stored, and all the corruptions of data are
3397 detected.

3398 **Assessment evidence**

3399 1. Logs of determination of type of data and corruptions of data
3400

3401 [\[AC-FIST\]](#) Assessment criteria: Formal proof of enforcement of integrity of data stored on the product3402 **Assessment reference**3403 Mitigation [MI-FIST](#).3404 **Assessment objective**

3405 Integrity of data

3406 **Assessment activities**

3407 1. Review the tool selection and configuration criteria documented by the manufacturer, the source code for the
3408 product, the formal definition of integrity, and the formal argument that it applies to a formalization of the
3409 product's source code

3410 **Assessment verdict**

3411 The verdict fail is assigned if any of the following conditions apply:

3412 1. The tool selection or configuration criteria are not documented, or the formal definition of integrity does not
3413 demonstrate the enforcement of integrity of data stored on the product, or the formal verification tool does not
3414 successfully output a proof.

3415 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

3416 1. The tool selection and configuration criteria are documented, the formal definition of integrity demonstrates
3417 the enforcement of integrity of data stored on the product, the formal verification tool successfully outputs a
3418 proof that the integrity statement is satisfied by the product.

3419 **Assessment evidence**

3420 1. The documentation documenting the tool selection and configuration criteria, how the tool is run, the source
3421 code for the product, the formal definition of the integrity, and the formal argument that it applies to a
3422 formalization of the product's source code

3423

3424 [\[AC-INTS\]](#) Assessment criteria: Cryptographic integrity protection of stored data3425 **Assessment reference**3426 Mitigation [MI-INTS](#).3427 **Assessment objective**

3428 Protect the integrity of stored integrity-sensitive data using a cryptographic integrity mechanism.

3429 **Assessment preparation**

- 3430 1. List all categories of data stored by the operating system for which unauthorized modification would lead to a
 3431 security incident, including boot components such as the bootloader and kernel image, kernel modules and
 3432 device drivers, operating-system-provided libraries, configuration stores holding critical security parameters,
 3433 certificate stores and trust anchors, credential and cryptographic-key stores, and audit and log files whose
 3434 forensic value depends on their integrity.
- 3435 2. Documentation describing the cryptographic integrity mechanism applied to each category of stored integrity-
 3436 sensitive data is available, including the algorithm used, the verification key or trust anchor used, and the
 3437 verification behaviour applied when an integrity check fails.

3438 **Assessment activities**

- 3439 1. Review the documentation to verify that every category of integrity-sensitive stored data is associated with a
 3440 documented cryptographic integrity mechanism conforming to TR-CRYP.
- 3441 2. Inspect the operating system in its operational state and verify that the documented cryptographic integrity
 3442 mechanism is applied to each category of integrity-sensitive stored data and that the cryptographic algorithm in
 3443 use matches the documentation and conforms to TR-CRYP.
- 3444 3. For each category of integrity-sensitive stored data, modify the stored data bypassing the operating system's
 3445 authorization mechanism and verify that the operating system detects the modification on the basis of the
 3446 cryptographic integrity mechanism and applies the documented failure behaviour.

3447 **Assessment verdict**

3448 The verdict fail is assigned if any of the following conditions apply:

- 3449 1. Documentation does not associate every category of integrity-sensitive stored data with a cryptographic
 3450 integrity mechanism, or any documented mechanism does not conform to TR-CRYP.
- 3451 2. The cryptographic integrity mechanism is not applied to any category of integrity-sensitive stored data, or the
 3452 algorithm in use does not conform to TR-CRYP.
- 3453 3. The operating system does not detect any modification of the stored data, or does not apply the documented
 3454 failure behaviour.

3455 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3456 1. Documentation associates every category of integrity-sensitive stored data with a cryptographic integrity
 3457 mechanism conforming to TR-CRYP.
- 3458 2. The cryptographic integrity mechanism is applied to every category of integrity-sensitive stored data and the
 3459 algorithm in use conforms to TR-CRYP.
- 3460 3. The operating system detects every modification of the stored data and applies the documented failure
 3461 behaviour.

3462 **Assessment evidence**

- 3463 1. Documentation listing every category of integrity-sensitive stored data and the cryptographic integrity
 3464 mechanism applied to each.
- 3465 2. Test results showing the cryptographic integrity mechanism applied to each category of integrity-sensitive
 3466 stored data and the algorithm in use.
- 3467 3. Test results showing detection of modification of stored data and the failure behaviour applied.

3468

3469

7.15 TR-IDTX: Integrity of data transmitted by the product

3470 [\[AC-DCTX\]](#) Assessment criteria: Detect corruption of data transmitted by the product

3471 **Assessment reference**3472 Mitigation [MI-DCTX](#).3473 **Assessment objective**

3474 Integrity of data

3475 **Assessment preparation**3476 1. List all types of data that may be transmitted by the product whose corruption should be detected and the
3477 corruption detection mechanism documented by the manufacturer for each type3478 **Assessment activities**

3479 1. For each type of data and method of detecting corruption, corrupt the data in a way that the method will detect

3480 **Assessment verdict**

3481 The verdict fail is assigned if any of the following conditions apply:

3482 1. Any method of detecting corruption does not match the type of the data transmitted, or any corruption of data
3483 is not detected.

3484 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

3485 1. All methods of detecting corruption match the type of the data transmitted, and all the corruptions of data are
3486 detected.3487 **Assessment evidence**3488 1. Logs of determination of type of data and corruptions of data
34893490 [\[AC-INTT\]](#) Assessment criteria: Cryptographic integrity protection of transmitted data3491 **Assessment reference**3492 Mitigation [MI-INTT](#).3493 **Assessment objective**

3494 Protect the integrity of transmitted integrity-sensitive data using a cryptographic integrity mechanism.

3495 **Assessment preparation**3496 1. List all categories of data transmitted by the operating system for which unauthorized modification in transit
3497 would lead to a security incident, including data transmitted through operating-system-provided network
3498 protocols (such as TLS, SSH, IPsec, and DNSSEC client or server implementations), remote administration
3499 interfaces, remote filesystem and file sharing protocols, remote logging and audit streams, and remote
3500 management or telemetry channels.3501 2. Documentation describing the cryptographic integrity mechanism applied to each category of transmitted
3502 integrity-sensitive data is available, including the algorithm used, the keying material or signing key used, and
3503 the verification behaviour applied by the receiver.3504 **Assessment activities**3505 1. Review the documentation to verify that every category of integrity-sensitive transmitted data is associated
3506 with a documented cryptographic integrity mechanism conforming to TR-CRYP.3507 2. Inspect the operating system in its operational state while it transmits data in each documented category.
3508 Confirm that the documented cryptographic integrity mechanism is applied to the transmitted data and that the
3509 cryptographic algorithm in use matches the documentation and conforms to TR-CRYP.3510 3. For each category of integrity-sensitive transmitted data, modify the data in transit between the product and the
3511 receiving endpoint and verify that the receiving endpoint rejects the modified data on the basis of the
3512 cryptographic integrity mechanism.3513 **Assessment verdict**

3514 The verdict fail is assigned if any of the following conditions apply:

- 3515 1. Documentation does not associate every category of integrity-sensitive transmitted data with a cryptographic
3516 integrity mechanism, or any documented mechanism does not conform to TR-CRYP.
- 3517 2. The cryptographic integrity mechanism is not applied to any category of integrity-sensitive transmitted data, or
3518 the algorithm in use does not conform to TR-CRYP.
- 3519 3. The receiving endpoint accepts any modification of the transmitted data.

3520 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3521 1. Documentation associates every category of integrity-sensitive transmitted data with a cryptographic integrity
3522 mechanism conforming to TR-CRYP.
- 3523 2. The cryptographic integrity mechanism is applied to every category of integrity-sensitive transmitted data and
3524 the algorithm in use conforms to TR-CRYP.
- 3525 3. The receiving endpoint rejects every modification of the transmitted data.

3526 **Assessment evidence**

- 3527 1. Documentation listing every category of integrity-sensitive transmitted data and the cryptographic integrity
3528 mechanism applied to each.
- 3529 2. Test results showing the cryptographic integrity mechanism applied to each category of transmitted integrity-
3530 sensitive data and the algorithm in use.
- 3531 3. Test results showing that modified transmitted data is rejected by the receiving endpoint.
3532

3533 7.16 TR-DMIN: Data Minimization

3534 [\[AC-DJST\]](#) Assessment criteria: Document and justify processed data

3535 **Assessment reference**

3536 Mitigation [MI-DJST](#).

3537 **Assessment objective**

3538 Minimize data processed

3539 **Assessment preparation**

- 3540 1. List all potential sources of data for the product. For each source of data, identify a method to detect whether
3541 the product is processing data from that source.

3542 **Assessment activities**

- 3543 1. Using the list of sources of data, and the method to detect whether the product is processing data from that
3544 source, list all sources of data processed. Compare to the documented list.

3545 **Assessment verdict**

3546 The verdict fail is assigned if any of the following conditions apply:

- 3547 1. Any source of processed data is not documented or lacks rationale.

3548 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3549 1. All sources of processed data are documented, including rationale.

3550 **Assessment evidence**

- 3551 1. List of sources of data, documentation of each source of data, list of sources of data processed, connection
3552 between each discovered source of processed data to its documentation
3553

3554 7.17 TR-AVAI: Availability

3555 [\[AC-AVNT\]](#) Assessment criteria: Availability of network services

3556 **Assessment reference**

3557 Mitigation [MI-AVNT](#).

3558 **Assessment objective**

3559 Protect availability of network functions

3560 **Assessment preparation**

3561 1. List all network services and identify essential and core network services

3562 **Assessment activities**3563 1. For each essential or core network service, examine the documentation for the denial-of-service mitigations the
3564 manufacturer has documented for each service3565 **Assessment verdict**

3566 The verdict fail is assigned if any of the following conditions apply:

3567 1. Any essential or core network service is not documented, or any mitigation is not documented by the
3568 manufacturer

3569 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

3570 1. Every essential or core network service is documented and the mitigations are documented by the
3571 manufacturer3572 **Assessment evidence**3573 1. All configuration files for network services, documentation of network services and the ways to mitigate a
3574 denial-of-service attack on it, internal lists of listening ports, results of an external port scan

3575

3576 [\[AC-WDOG\]](#) Assessment criteria: Watchdog and self-initiated reset3577 **Assessment reference**3578 Mitigation [MI-WDOG](#).3579 **Assessment objective**

3580 Availability

3581 **Assessment preparation**

3582 1. Document the conditions that indicate the product cannot perform its functions

3583 **Assessment activities**

3584 1. Cause each of the conditions to occur and observe whether the product resets

3585 **Assessment verdict**

3586 The verdict fail is assigned if any of the following conditions apply:

3587 1. Not every condition triggers an automatic reset

3588 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

3589 1. Every condition triggers an automatic reset

3590 **Assessment evidence**

3591 1. Documentation, log messages

3592

3593 [\[AC-RTDL\]](#) Assessment criteria: Real-time deadline preservation3594 **Assessment reference**3595 Mitigation [MI-RTDL](#).3596 **Assessment objective**

3597 Ensure security mechanisms do not compromise real-time availability

3598 **Assessment preparation**

3599 1. List all real-time tasks and their documented worst-case execution times

3600 **Assessment activities**

3601 1. Run documented real-time tasks concurrently with security-relevant operations (e.g. MPU fault handling,
3602 integrity verification, cryptographic operations). Measure the worst-case execution time of each real-time task
3603 under this load.

3604 **Assessment verdict**

3605 The verdict fail is assigned if any of the following conditions apply:

3606 1. Any real-time task exceeds its documented worst-case execution time.

3607 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

3608 1. Every real-time task completes within its documented worst-case execution time.

3609 **Assessment evidence**

3610 1. Timing measurements, task execution logs, documented worst-case execution time specifications.

3611

3612 [\[AC-RTRY\]](#) Assessment criteria: Retry and degraded behaviour on unavailability of the remote data processing
3613 solution

3614 **Assessment reference**

3615 Mitigation [MI-RTRY](#).

3616 **Assessment objective**

3617 Detect and recover from unavailability of the remote data processing solution

3618 **Assessment preparation**

3619 1. Documentation describing the timeout, retry, and degraded-behaviour mechanisms used for communication
3620 with each remote data processing solution is available.

3621 2. The product is in operational state with remote data processing solution connectivity configured.

3622 **Assessment activities**

3623 1. Review the documentation to identify the timeout controls, retry interval, and defined behaviour applied on
3624 prolonged unavailability for each remote data processing solution.

3625 2. Block connectivity to the remote data processing solution and monitor the product's behaviour. Verify that the
3626 product detects the unavailability, retries within 24 hours, and applies the defined behaviour for the dependent
3627 product function after the timeout expires.

3628 **Assessment verdict**

3629 The verdict fail is assigned if any of the following conditions apply:

3630 1. Documentation does not describe timeout controls, retry behaviour, or defined behaviour on prolonged
3631 unavailability.

3632 2. The product fails to detect unavailability, fails to retry within 24 hours, or does not apply the defined behaviour
3633 on prolonged unavailability.

3634 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

3635 1. Documentation describes timeout controls, retry within 24 hours, and a defined behaviour on prolonged
3636 unavailability for each remote data processing solution.

3637 2. The product detects unavailability, retries within 24 hours, and applies the defined behaviour on prolonged
3638 unavailability.

3639 **Assessment evidence**

3640 1. Documentation describing timeout, retry, and degraded-behaviour mechanisms.

3641 2. Test results showing detection, retry attempts, and degraded behaviour.

3642

3643 7.18 TR-LMAS: Minimize exposed interfaces

3644 [\[AC-JSTY\]](#) Assessment criteria: Document and justify exposed interfaces

3645 **Assessment reference**

3646 Mitigation [MI-JSTY](#).

3647 **Assessment objective**

3648 Limit attack surface

3649 **Assessment preparation**

3650 1. List all types of interfaces on the product that may be exposed to an attacker, whether enabled or disabled. For
 3651 each type of interface, identify a method to list all exposed interfaces of that type. List all states of the product
 3652 with different exposed interfaces of the product in its secure-by-default configuration, including but not limited
 3653 to initial configuration, startup, in use, idle, shutdown, and reset, if applicable. For each distinct exposed
 3654 interface in each state, describe the interface and why it has to be enabled by default.

3655 **Assessment activities**

3656 1. Using the list of types of interfaces, the list of states of the product, and the method to list all exposed
 3657 interfaces of that type, list all exposed interfaces in each state. Compare to the documented list.

3658 **Assessment verdict**

3659 The verdict fail is assigned if any of the following conditions apply:

3660 1. Not all discovered interfaces are documented, including rationale

3661 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

3662 1. All discovered interfaces are documented, including rationale

3663 **Assessment evidence**

3664 1. List of types of interfaces, list of product states, documentation of each exposed interface, output of methods to
 3665 list all exposed interfaces, connection between each discovered interface to its documentation
 3666

3667 7.19 TR-LOGG: Logging and monitoring

3668 [\[AC-LOGG\]](#) Assessment criteria: Logging

3669 **Assessment reference**

3670 Mitigation [MI-LOGG](#).

3671 **Assessment objective**

3672 Monitoring and recording security-relevant events

3673 **Assessment preparation**

3674 1. List all types of security-relevant internal events, including at minimum authentication successes and failures,
 3675 changes to configuration or to privilege assignments, access to or modification of security-relevant data, and
 3676 access to or modification of security-relevant functions

3677 **Assessment activities**

3678 1. For each type of security-relevant internal event, trigger the event

3679 **Assessment verdict**

3680 The verdict fail is assigned if any of the following conditions apply:

3681 1. For any triggered event, the log does not contain a message indicating the event, or the log message includes
 3682 information likely to be confidential

3683 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3684 1. For each triggered event, the log contains a message indicating the event, log message does not include any
3685 information likely to be confidential

3686 **Assessment evidence**

- 3687 1. Method of triggering events, log messages with annotations

3688 NOTE: Guidance: One type of event whose log message must take care to not accidentally include a secret is
3689 failed password authentication attempts. Since people often type their password into the username field,
3690 including the username field in the log message may result in including a secret in the log message.

3691

3692 **7.20 TR-SCDL: Secure deletion**

3693 [\[AC-RSET\]](#) Assessment criteria: Secure deletion via reset

3694 **Assessment reference**

3695 Mitigation [MI-RSET](#).

3696 **Assessment objective**

3697 Secure deletion

3698 **Assessment preparation**

- 3699 1. Document every kind of stored data or setting that may be changed by the user on the product, how to store it
3700 on the product, and how to read it from the product

3701 **Assessment activities**

- 3702 1. For each kind of user data or setting that may be stored and changed by the user on the product, write an
3703 instance of the data or setting stored on the product that is different from the default and read it from the
3704 product; once all kinds of data have been written and read, power cycle or reset the product, and read each kind
3705 of data again

3706 **Assessment verdict**

3707 The verdict fail is assigned if any of the following conditions apply:

- 3708 1. Any data or setting is the same for both of the reads

3709 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3710 1. No data or setting is the same for both of the reads

3711 **Assessment evidence**

- 3712 1. Record of each type of data or setting, what data or setting was written, what data or setting was returned by
3713 the first read, and what data or setting was returned by the second read, comparison of each one
3714

3715 [\[AC-INST\]](#) Assessment criteria: Secure deletion via reinstallation

3716 **Assessment reference**

3717 Mitigation [MI-INST](#).

3718 **Assessment objective**

3719 Secure deletion

3720 **Assessment preparation**

- 3721 1. Document every kind of data or setting that may be stored and changed by the user on the product, how to
3722 store it on the product, and how to read it from the product

3723 **Assessment activities**

- 3724 1. For each kind of user data or setting that may be stored and changed by the user on the product, write an
3725 instance of the data or setting stored on the product that is different from the default and read it from the

3726 product; once all kinds of data have been written and read, reinstall the product with the secure delete option,
3727 and read the data or settings again

3728 **Assessment verdict**

3729 The verdict fail is assigned if any of the following conditions apply:

3730 1. Any data or setting is the same for both of the reads

3731 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

3732 1. No data or setting is the same for both of the reads

3733 **Assessment evidence**

3734 1. Record of each type of data or setting, what data or setting was written, what data or setting was returned by
3735 the first read, and what data or setting was returned by the second read, comparison of each one

3736

3737 [\[AC-DELE\]](#) Assessment criteria: Secure deletion via secure deletion function

3738 **Assessment reference**

3739 Mitigation [MI-DELE](#).

3740 **Assessment objective**

3741 Secure deletion

3742 **Assessment preparation**

3743 1. Document every kind of data or setting that may be stored and changed by the user on the product, how to
3744 store it on the product, and how to read it from the product

3745 **Assessment activities**

3746 1. For each kind of user data or setting that may be stored and changed by the user on the product, write an
3747 instance of the data or setting stored on the product that is different from the default and read it from the
3748 product; once all kinds of data have been written and read, activate the secure deletion function, and read the
3749 data or settings again

3750 **Assessment verdict**

3751 The verdict fail is assigned if any of the following conditions apply:

3752 1. Any data or setting is the same for both of the reads

3753 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

3754 1. No data or setting is the same for both of the reads

3755 **Assessment evidence**

3756 1. Record of each type of data or setting, what data or setting was written, what data or setting was returned by
3757 the first read, and what data or setting was returned by the second read, comparison of each one

3758

3759 **7.21 TR-SDTR: Secure data read and transfer**

3760 [\[AC-SDRF\]](#) Assessment criteria: Secure data read from product

3761 **Assessment reference**

3762 Mitigation [MI-SDRF](#).

3763 **Assessment objective**

3764 Secure data read

3765 **Assessment preparation**

3766 1. List all data and settings

3767 **Assessment activities**

- 3768 1. For each kind of data or setting, read the data or setting as an authorized user, then attempt read the data or
3769 setting as an unauthorized user, if any exists

3770 **Assessment verdict**

3771 The verdict fail is assigned if any of the following conditions apply:

- 3772 1. Not all data and settings can be read by the authorized user, or any data or setting can be read by an
3773 unauthorized user

3774 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3775 1. All data and settings can be read by the authorized user, and no data or setting can be read by an unauthorized
3776 user

3777 **Assessment evidence**

- 3778 1. List of data and settings, log message showing success or failure of each read by the authorized user and, if
3779 applicable, the unauthorized user

3780

3781 [\[AC-SDTR\]](#) Assessment criteria: Secure data transfer to another product

3782 **Assessment reference**

3783 Mitigation [MI-SDTR](#).

3784 **Assessment objective**

3785 Secure data transfer

3786 **Assessment preparation**

- 3787 1. Prepare methods by which an unauthorized user could read the data during transfer as outlined in the risk
3788 assessment

3789 **Assessment activities**

- 3790 1. Read the data or settings, initiate the data transfer, attempt to read or alter the transferred data and settings as
3791 an unauthorized user, read the new data and settings on the target product

3792 **Assessment verdict**

3793 The verdict fail is assigned if any of the following conditions apply:

- 3794 1. Any data or settings could be read or altered by an unauthorized user, or the data and settings read from the
3795 original product and target product are not the same wherever technically possible

3796 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3797 1. No data or settings could be read or altered by an unauthorized user, and the data and settings read from the
3798 original product and target product are the same wherever technically possible

3799 **Assessment evidence**

- 3800 1. List of data and settings, log messages from the attempts to read or alter data as the unauthorized user, data and
3801 settings as read from the source product and as read from the target product, comparison explaining technical
3802 reasons for any differences in the two versions

3803

3804 **7.22 TR-VULH: Vulnerability handling**

3805 [\[AC-VULH-1\]](#) Assessment criteria: Enabling Vulnerability Handling in Integrated Products

3806 **Assessment reference**

3807 Mitigation [MI-VULH-1](#).

3808 **Assessment objective**

3809 Vulnerability handling

3810 **Assessment activities**

- 3811 1. Review product's SBOM for detailed lists of third-party components and verify the accuracy of identifiers of
3812 those components. If applicable and permissible, apply scanning and analysis techniques to the product to
3813 verify that the supplied SBOM is accurate and complete.

3814 **Assessment verdict**

3815 The verdict fail is assigned if any of the following conditions apply:

- 3816 1. Product's SBOM does not contain accurate identifiers for third-party components or unlisted third-party
3817 components are discovered through product inspection

3818 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3819 1. Product's SBOM contains accurate identifiers for third-party components which can be verified from the
3820 sources documented by the manufacturer, and unlisted third-party components are not discovered through
3821 product inspection

3822 **Assessment evidence**

- 3823 1. Logs from product analysis and comparison to supplied SBOM
3824
3825

3826

Annex A (informative):

3827

Mapping between the present document and CRA

3828

requirements

3829

Editor's Note: This table maps the essential cybersecurity requirements from Annex I of Regulation (EU) 2024/2847

3830

[i.1] to the technical security requirements in clause 5 of the present document. The "Clause(s) of the present

3831

document" column uses TR-XXX identifiers pending the restructuring of chapter 5 to match the common CRA vertical

3832

hEN skeleton clause numbering.

No	Description	Requirements of Regulation	Clause(s) of the present document	U/C	Condition
1	Annex I, Part 1, (1)	Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.	TR-SSDD, TR-LMII	C	See mapping table on the applicability of the technical cybersecurity requirements in clause 5.1
2	Annex I, Part 1, (2)(a)	Products with digital elements shall be made available on the market without known exploitable vulnerabilities.	TR-NKEV	U/C	
3	Annex I, Part 1, (2)(b)	Products with digital elements shall be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state.	TR-SDEF	U/C	
4	Annex I, Part 1, (2)(c)	Products with digital elements shall ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them.	TR-SCUD	U/C	
5	Annex I, Part 1, (2)(d)	Products with digital elements shall ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access.	TR-AUTH	U/C	
6	Annex I, Part 1, (2)(e)	Products with digital elements shall protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by best practice mechanisms, and by using other technical means.	TR-MISO, TR-LMII, TR-CDST, TR-CDTX, TR-CRYP	U/C	
7	Annex I, Part 1, (2)(f)	Products with digital elements shall protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions.	TR-MISO, TR-IDST, TR-IDTX	U/C	

8	Annex I, Part 1, (2)(g)	Products with digital elements shall process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation).	TR-DMIN	U/C
9	Annex I, Part 1, (2)(h)	Products with digital elements shall protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks.	TR-AVAI, TR-LMII	U/C
10	Annex I, Part 1, (2)(i)	Products with digital elements shall minimise the negative impact by the products themselves or connected products on the availability of services provided by other products or networks.	TR-MINI, TR-SDEF, TR-AVAI, TR-SSDD, TR-LMII	U/C
11	Annex I, Part 1, (2)(j)	Products with digital elements shall be designed, developed and produced to limit attack surfaces, including external interfaces.	TR-MISO, TR-LMAS, TR-SSDD, TR-LMII	U/C
12	Annex I, Part 1, (2)(k)	Products with digital elements shall be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques.	TR-MISO, TR-LMII, TR-AVAI, TR-SSDD	U/C
13	Annex I, Part 1, (2)(l)	Products with digital elements shall provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user.	TR-LOGG	U/C
14	Annex I, Part 1, (2)(m)	Products with digital elements shall provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.	TR-SCDL, TR-SDTR	U/C
15	Annex I, Part 2	Essential cybersecurity requirements relating to the vulnerability handling processes.	TR-VULH	U

3834 Annex B (informative): 3835 Risk identification and assessment methodology

3836 This annex describes how the security requirements in clause 5 are derived from a structured risk assessment. Assets,
3837 product functions, risk factors, assumptions, and threats are described in clauses B.1 through B.4. Each threat lists the
3838 requirements that mitigate it. The mapping of use cases to risk factors in clause B.5 and the security profiles in clause
3839 B.6 together determine which mitigations apply to a given product.

3840 B.1 Assets

3841 B.1.1 Data assets

- 3842 • User data (documents, media, application state)
- 3843 • Logs (system logs, security audit logs, application logs)
- 3844 • Credentials and keys (passwords, API keys, cryptographic keys, tokens)
- 3845 • Certificates (TLS certificates, code-signing certificates, root CA stores)
- 3846 • Configuration files (system configuration, service configuration, security policies)

3847 B.1.2 Software assets

- 3848 • Kernel (including kernel modules)
- 3849 • System libraries and runtime components
- 3850 • Applications and system services
- 3851 • Device drivers
- 3852 • Boot firmware and bootloader
- 3853 • Firmware images (update packages, recovery images)

3854 B.1.3 Hardware-interfacing assets

- 3855 • Memory (system memory, memory-mapped I/O)
- 3856 • Storage (internal storage, removable media)
- 3857 • Processing units (CPUs, co-processors, GPUs)
- 3858 • Peripheral interfaces (USB, PCI, SPI, I2C, GPIO)
- 3859 • Network interfaces (Ethernet, Wi-Fi, Bluetooth, cellular)
- 3860 • Debug and management interfaces (JTAG, SWD, serial console, BMC)

3861 B.1.4 Network assets

- 3862 • Network services (listening services, exposed APIs)
- 3863 • Active connections (established sessions, tunnels)
- 3864 • Routing and firewall state (routing tables, firewall rules, NAT state)
- 3865 • DNS resolution (resolver configuration, cached entries)

3866 B.1.5 Identity and access assets

- 3867 • User accounts and administrator accounts
- 3868 • Sessions (active login sessions, authentication tokens)
- 3869 • Access control policies (file permissions, mandatory access control rules, capability sets)

3870 B.1.6 Product functions

- 3871 • Resource allocation (memory management, scheduling, storage quotas, other resource usage limits)
- 3872 • Isolation (memory protection, storage protection, other permissions)
- 3873 • Abstract I/O (network stack, file systems, video, sound, input devices)
- 3874 • Hardware communication (device drivers)
- 3875 • Power management
- 3876 • Hardware management
- 3877 • Configuration (software to run, hardware configuration, I/O configuration)
- 3878 • Initialization (initialize hardware, start software services)
- 3879 • Authentication
- 3880 • Authorization
- 3881 • Software management (software verification, software installation, security updates, software upgrade,
3882 software removal, firmware upgrades, load kernel modules)
- 3883 • Logging
- 3884 • Monitoring and notifications

3885 B.1.7 Impact of asset compromise

3886 The following summarises the potential impact when assets from each category are compromised in terms of
3887 confidentiality, integrity, and availability.

- 3888 • **Data assets:** loss of confidentiality exposes user data, credentials, or keys to unauthorized parties. Loss of
3889 integrity allows an attacker to modify configuration or inject false log entries. Loss of availability prevents the
3890 product from accessing data it needs to function.
- 3891 • **Software assets:** loss of integrity allows an attacker to modify the kernel, libraries, or firmware, potentially
3892 gaining persistent control of the product. Loss of availability prevents the product from starting or operating.
- 3893 • **Hardware-interfacing assets:** loss of confidentiality of memory contents exposes sensitive data. Loss of
3894 integrity of debug interfaces allows unauthorized code execution. Loss of availability of storage or network
3895 interfaces degrades product functions.
- 3896 • **Network assets:** loss of confidentiality of active connections exposes transmitted data. Loss of integrity of
3897 routing or firewall state allows traffic redirection or bypass. Loss of availability of network services denies
3898 service to users.
- 3899 • **Identity and access assets:** loss of confidentiality of accounts or sessions enables impersonation. Loss of
3900 integrity of access control policies allows privilege escalation. Loss of availability of authentication locks out
3901 legitimate users.
- 3902 • **Product functions:** loss of integrity of isolation, resource allocation, or authorization functions undermines the
3903 security guarantees that other mitigations depend on. Loss of availability of any core function is a denial-of-
3904 service condition.

3905 B.2 Risk factors

3906 B.2.1 General comments regarding risk factors

3907 Risk factors determine which mitigation(s) satisfy each of the technical requirements in clause 5.2.

3908 Manufacturers determine the level of each risk factor via the development of a threat model and risk profile based on
3909 the intended and foreseeable use and misuse of the operating system.

3910 Risk factors may increase the likelihood of an incident, increase the impact of an incident, or both. As a result, different
3911 mitigation strategies may be more or less relevant to different risk factors.

3912 The overall risk related to each use case should be considered, and is calculated by combining risk factors affecting both
3913 likelihood and impact of an incident.

3914 B.2.2 RF-NUSR: Number of User Accounts

3915 The number of user accounts of end-users expected on the system, excluding administrator accounts.

- 3916 • NUSR-0: foreseeable use does not include user accounts for end-users
- 3917 • NUSR-1: foreseeable use is only one user account for an end-user
- 3918 • NUSR-2: foreseeable use of the operating system is multiple user accounts for end-users

3919 B.2.3 RF-CUSR: User Account Concurrency

3920 The number of user accounts expected to use the system concurrently, including administrator accounts if they are
3921 configurable or accessible by end-users.

- 3922 • CUSR-0: foreseeable use is one authenticated end-user using the device at a time, including authentication by
3923 physical access
- 3924 • CUSR-1: foreseeable use of the operating system is small number of authenticated users simultaneously active
3925 on the operating system who are trusted not to actively attempt to compromise the system
- 3926 • CUSR-2: foreseeable use of the operating system is multiple authenticated untrusted users simultaneously
3927 active on the operating system

3928 B.2.4 RF-PPII: Potential for Collection of Personally Identifiable Information

3929 Potential for collection of personally identifiable information about an individual person.

- 3930 • PPII-0: foreseeable use includes no or incidental collection of PII
- 3931 • PPII-1: foreseeable use includes collection of moderate amounts of PII
- 3932 • PPII-2: foreseeable use includes collection of extensive amounts of PII by default

3933 B.2.5 RF-SNDS: Sensitivity of Data Stored

3934 Sensitivity of data stored, as measured by impact of loss of its integrity, confidentiality, or availability.

- 3935 • SNDS-0: foreseeable use includes no or incidental storage of sensitive data
- 3936 • SNDS-1: foreseeable use includes storing moderate amounts of sensitive data
- 3937 • SNDS-2: foreseeable use includes storing extensive amounts of sensitive data by default

3938 B.2.6 RF-SNDT: Sensitivity of Data Transmitted

3939 Sensitivity of data transmitted, as measured by impact of loss of its integrity, confidentiality, or availability.

- 3940 • SNDT-0: foreseeable use includes no or incidental transmission of sensitive data
- 3941 • SNDT-1: foreseeable use includes transmission of moderate amounts of sensitive data

- 3942 • SNDT-2: foreseeable use includes transmission of extensive amounts of sensitive data by default

3943 B.2.7 RF-SENF: Sensitivity of Functions

3944 Sensitivity of functions of device, as measured by impact of loss of its integrity, confidentiality, or availability.

- 3945 • SENF-0: foreseeable use includes no or incidental provision of sensitive functions
- 3946 • SENF-1: foreseeable use may provide arbitrary sensitive functions
- 3947 • SENF-2: foreseeable use provides sensitive functions by default

3948 B.2.8 RF-PHYS: Physical Access by Threat Actors to the Device

3949 Exposure of the device to physical access by users.

- 3950 • PHYS-0: foreseeable use is only in environments without physical exposure to untrusted users
- 3951 • PHYS-1: foreseeable use includes incidental physical exposure to untrusted users
- 3952 • PHYS-2: foreseeable use includes regular physical exposure to untrusted users

3953 B.2.9 RF-UEIN: Processing of Untrusted External Inputs

3954 Exposure to untrusted external inputs that are processed by the platform.

- 3955 • UEIN-0: only used in environments without processing of untrusted external inputs
- 3956 • UEIN-1: may incidentally process untrusted external inputs
- 3957 • UEIN-2: used primarily to process untrusted external inputs

3958 B.2.10 RF-LOSS: Probability of Loss of the Device

3959 Likelihood of loss or theft of the device, allowing threat actors unlimited physical access to the device.

- 3960 • LOSS-0: foreseeable use is in a device with no or incidental loss likelihood
- 3961 • LOSS-1: foreseeable use is in a device with moderate loss likelihood
- 3962 • LOSS-2: foreseeable use is in a device with a high loss likelihood, such as devices which are common targets
3963 of theft such as mobile phones

3964 B.2.11 RF-HWMD: Hardware Modifiability by End Users

3965 Likelihood that the hardware of the platform will be changed from its secure-by-default state.

- 3966 • HWMD-0: foreseeable use limited to devices with hardware that is not modifiable by end-users
- 3967 • HWMD-1: foreseeable use includes hardware modifications by skilled administrators
- 3968 • HWMD-2: foreseeable use includes hardware modification by unskilled users

3969 B.2.12 RF-SWMD: Software Modifiability by End Users

3970 Likelihood that the software on the platform (including firmware) will be changed from its secure-by-default state.

- 3971 • SWMD-0: foreseeable use only allows the installation of trusted and verified software, such as updates
- 3972 • SWMD-1: foreseeable use allows for the installation of arbitrary software or for substantial modification of
3973 pre-installed software
- 3974 • SWMD-2: foreseeable use actively encourages and facilitates the installation of frequently malicious software

3975 B.2.13 RF-DVCS: Untrusted Peripheral Devices

3976 Likelihood of untrusted peripheral devices being attached to the platform via a connection that is a plausible attack
3977 vector, such as by USB or PCI bus.

- 3978 • DVCS-0: foreseeable use has no accessible peripheral ports
- 3979 • DVCS-1: foreseeable use includes only trusted and safe peripheral devices
- 3980 • DVCS-2: foreseeable use allows for arbitrary peripheral device attachment

3981 B.2.14 RF-TNET: Access to a Public Network

3982 Likelihood that the device will initiate connections to public networks.

- 3983 • TNET-0: foreseeable use has no mechanism to reasonably connect to a public network
- 3984 • TNET-1: foreseeable use allows internet access for only highly restricted functions, such as retrieving security
3985 updates
- 3986 • TNET-2: foreseeable use allows for arbitrary access to a public network, such as by browsing the web

3987 B.2.15 RF-FNET: Accessed From Untrusted Networks Including a Public 3988 Network

3989 Likelihood that the device will be exposed to incoming traffic from public networks.

- 3990 • FNET-0: foreseeable use is limited to trusted and private networks
- 3991 • FNET-1: foreseeable use includes untrusted local networks but not the open internet
- 3992 • FNET-2: foreseeable use includes being connected directly to the open internet

3993 B.2.16 RF-CONF: Configurability

3994 Degree of security-relevant configuration change of the operating system necessary for use.

- 3995 • CONF-0: foreseeable use does not require storing operating system configuration changes
- 3996 • CONF-1: foreseeable use involves operating system configuration changes only by skilled administrators
- 3997 • CONF-2: foreseeable use of the operating system includes configuration changes by end-users

3998 B.2.17 RF-ADMN: Administration

3999 Availability and skill of administrators.

- 4000 • ADMN-0: foreseeable use does not require administration
- 4001 • ADMN-1: foreseeable use always has skilled administrators available on call
- 4002 • ADMN-2: foreseeable use may involve unskilled administrators

4003 B.2.18 RF-SUPP: Support and Foreseeable Updates

4004 How long the product is expected to be in use, and whether the product is expected to be updated throughout its life
4005 cycle.

- 4006 • SUPP-0: foreseeable use does not require that the operating system be updated at any point in its lifecycle
- 4007 • SUPP-1: foreseeable use includes the installation of updates by end-users with access to the operating system
- 4008 • SUPP-2: foreseeable use necessitates that the manufacturer provide frequent, automatic, and/or time-sensitive
4009 updates to the product, and may reasonably be expected to do so

4010 B.2.19 RF-RDPS: Remote data processing dependency

4011 Whether the product depends on one or more remote data processing solutions for product functions, as described in
4012 clause [4.8](#).

4013

- RDPS-0: the product does not depend on any remote data processing solution for any product function

4014

- RDPS-1: the product depends on one or more remote data processing solutions for at least one product
4015 function

4016 B.3 Assumptions

4017 Assumptions can be updated to be less stringent as more use cases and mitigations are added to the standard.

4018 B.3.1 AS-PP: Proper platform

4019 The platform the product runs on is trustworthy. The OS may choose to detect and/or correct hardware errors.

4020 B.3.2 AS-PA: Proper administrator

4021 The product administrator is not intentionally hostile and is engaging in good faith efforts to administer the system
4022 properly.

4023 B.3.3 AS-LP: Attacker has limited physical access to product

4024 An attacker will have only temporary physical access to the product.

4025 B.3.4 AS-LR: Attacker has limited resources

4026 An attacker has the resources available to a small group of skilled individuals, without the backing of large
4027 corporations, nation-states, or immense wealth.

4028 B.4 Security analysis

4029 B.4.1 General

4030 The approach to listing threats is to separate them by mitigation so that they may be associated with mitigations more
4031 directly.

4032 B.4.2 Risk assessment methodology

4033 Risk factor levels for each security profile (see clause B.6) are determined by reading the descriptions for each risk
4034 factor level (see clause B.2) and choosing the one that most accurately represents the highest risk for the use case.

4035 For each threat, a formula based on the risk factor levels is used to calculate the Likelihood and Impact of the threat, on
4036 a scale of Low, Medium, and High.

4037 For each threat, both likelihood and impact must be Low before the risk is considered sufficiently mitigated. If the
4038 calculated levels are not already Low, then mitigations must be applied until they are both Low. The mitigation sets that
4039 will accomplish this are listed in each threat description.

4040 B.4.3 TH-UEVU: Unknown exploitable vulnerabilities

4041 Attacker may use unknown exploitable vulnerabilities in the product implementation to get unauthorized access to
4042 product assets.

4043 Requirements that mitigate this threat: SSDD, SDEF, MSAF, LMII, LMAS, LOGG

4044 Mitigations for Likelihood:

4045

- Medium to Low: SSCA, SCFS, MMAC, ADEF

4046

- High to Low: SSCA, (FZ95 or BTIN or IMSL), SCFS, MMAC, ASLR, MSAF-*, MZRO-*, MRWX-*,
4047 NKAM, PULS, MRCO, ADEF, JSTY

Risk factors	Likelihood	Security profiles
none of NUSR, CUSR, SENF, PHYS, or FNET is above level 0	Low	LR, IoT-1
all others	Medium	IoT-2, IoT-3, WE-1
any of NUSR, CUSR, SENF, PHYS, or FNET is at level 2	High	RO-1, OT-1, MOB-1, PC-*, LA-*, PS-1, SE-*

4048 Mitigations for Impact:

- 4049 • Medium to Low: LOGG
- 4050 • High to Low: LOGG

Risk factors	Impact	Security profiles
none of SNDS, SNDT, or SENF is above level 0	Low	LR, IoT-1
the highest of SNDS, SNDT, and SENF is at level 1	Medium	IoT-2, IoT-3
any of SNDS, SNDT, or SENF is at level 2	High	RO-1, OT-1, MOB-1, WE-1, PC-*, LA-*, PS-1, SE-*

4051 B.4.4 TH-KEVU: Known exploitable vulnerabilities

4052 Attacker may use known exploitable vulnerabilities in the product implementation to get unauthorized access to product
4053 assets.

4054 Requirements that mitigate this threat: NKEV, SSDD, SDEF, MSAF, LMII, LMAS, LOGG

4055 All mitigations from TH-UEVU apply (using that requirement's risk formula), in addition to:

4056 Mitigations for Likelihood:

- 4057 • Medium to Low: (KEVD or KEVA), KEVM, (SUVP or SUAP or SUOE or SUA0), VULH
- 4058 • High to Low: KEVA, KEVM, (KEVT or SCAN), (SUAP or SUA0), VULH

Risk factors	Likelihood	Security profiles
ADMN is at level 0 or SUPP is at level 0	Low	LR, IoT-1
all others	Medium	WE-1
both ADMN and SUPP are at level 2	High	IoT-2, IoT-3, RO-1, OT-1, MOB-1, PC-*, LA-*, PS-1, SE-*

4059

Risk factors	Impact	Security profiles
none of SNDS, SNDT, or SENF is above level 0	Low	LR, IoT-1
the highest of SNDS, SNDT, and SENF is at level 1	Medium	IoT-2, IoT-3
any of SNDS, SNDT, or SENF is at level 2	High	RO-1, OT-1, MOB-1, WE-1, PC-*, LA-*, PS-1, SE-*

4060 B.4.5 TH-UAPP: Unauthorized access to product assets via unprotected 4061 physical interfaces in default configuration

4062 Attacker may use unprotected debug or management interfaces to get unauthorized access to product assets via physical
4063 access in the default configuration of the product.

4064 Requirements that mitigate this threat: SDEF, AUTH, ACCS, LMAS, LOGG

4065 Mitigations for Likelihood:

- 4066 • Medium to Low: PDDI-1, AUTH
- 4067 • High to Low: ADEF, PDDI-2, AUTH

Risk factors	Likelihood	Security profiles
PHYS is at level 0	Low	LR, IoT-1
all others	Medium	IoT-2, IoT-3, RO-1, PC-*, PS-1, SE-*
PHYS is above level 0 and any of SNDS, SNDT, or SENF is at level 2	High	OT-1, MOB-1, WE-1, LA-*

4068 Mitigations for Impact:

- 4069 • Medium to Low: LOGG
- 4070 • High to Low: JSTY, LOGG

Risk factors	Impact	Security profiles
none of SNDS, SNDT, or SENF is above level 0	Low	LR, IoT-1
the highest of SNDS, SNDT, and SENF is at level 1	Medium	IoT-2, IoT-3
any of SNDS, SNDT, or SENF is at level 2	High	RO-1, OT-1, MOB-1, WE-1, PC-*, LA-*, PS-1, SE-*

4071 **B.4.6 TH-UAPS: Unauthorized access to product assets via unprotected local**
 4072 **software access in default configuration**

4073 Attacker may use unprotected debug or management interfaces to get unauthorized access to product assets via local
 4074 software access in the default configuration of the product.

4075 Requirements that mitigate this threat: SDEF, AUTH, LCKT, CRED, ACCS, PRIV, SESS, LMAS, LOGG

4076 Mitigations for Likelihood:

- 4077 • Medium to Low: PDDI-1, AUTH, LCKT, CRED
- 4078 • High to Low: ADEF, PDDI-3, AUTH, LCKT, CRED, ACCS, PRIV, SESS

Risk factors	Likelihood	Security profiles
none of NUSR or SWMD is above level 0	Low	LR, IoT-*,
all others	Medium	RO-1, OT-1, WE-1
any of NUSR or SWMD is at level 2 and any of SNDS, SNDT, or SENF is at level 2	High	MOB-1, PC-*, LA-*, PS-1, SE-*

4079 Mitigations for Impact:

- 4080 • Medium to Low: LOGG
- 4081 • High to Low: JSTY, LOGG

Risk factors	Impact	Security profiles
none of SNDS, SNDT, or SENF is above level 0	Low	LR, IoT-1
the highest of SNDS, SNDT, and SENF is at level 1	Medium	IoT-2, IoT-3

any of SNDS, SNDT, or SENF is at level 2 High RO-1, OT-1, MOB-1, WE-1, PC-*, LA-*, PS-1, SE-*

4082 **B.4.7 TH-UAPN: Unauthorized access to product assets via unprotected**
 4083 **network interfaces in default configuration**

4084 Attacker may use unprotected debug or management interfaces to get unauthorized access to product assets via the
 4085 network in the default configuration of the product.

4086 Requirements that mitigate this threat: SDEF, AUTH, LCKT, CRED, ACCS, SESS, LMAS, LOGG

4087 Mitigations for Likelihood:

- 4088 • Medium to Low: PDDI-1, AUTH, LCKT, CRED
- 4089 • High to Low: ADEF, PDDI-4, AUTH, LCKT, CRED, ACCS, SESS

Risk factors	Likelihood	Security profiles
none of FNET or TNET is above level 0	Low	LR, IoT-1
all others	Medium	IoT-2, IoT-3
any of FNET or TNET is above level 0 and any of SNDS, SNDT, or SENF is at level 2	High	RO-1, OT-1, MOB-1, WE-1, PC-*, LA-*, PS-1, SE-*

4090 Mitigations for Impact:

- 4091 • Medium to Low: LOGG
- 4092 • High to Low: JSTY, LOGG

Risk factors	Impact	Security profiles
none of SNDS, SNDT, or SENF is above level 0	Low	LR, IoT-1
the highest of SNDS, SNDT, and SENF is at level 1	Medium	IoT-2, IoT-3
any of SNDS, SNDT, or SENF is at level 2	High	RO-1, OT-1, MOB-1, WE-1, PC-*, LA-*, PS-1, SE-*

4093 **B.4.8 TH-UADT: Unauthorized access to confidential data transmitted**

4094 Attacker may use network access to get unauthorized access to confidential data transmitted by the product.

4095 Requirements that mitigate this threat: CDTX, ENTX, CRYP, IDTX, INTT, DMIN

4096 Mitigations for Likelihood:

- 4097 • Medium to Low: RRDC
- 4098 • High to Low: CDTX, ENTX, CRYP, DCTX, INTT, RRDC

Risk factors	Likelihood	Security profiles
TNET is at level 0	Low	LR, IoT-1
TNET is at level 1	Medium	IoT-2, IoT-3, OT-1, WE-1
TNET is at level 2	High	RO-1, MOB-1, PC-*, LA-*, PS-1, SE-*

4099 Mitigations for Impact:

- 4100 • Medium to Low: DJST
- 4101 • High to Low: DJST

Risk factors	Impact	Security profiles
---------------------	---------------	--------------------------

SNDT is at level 0 Low LR, IoT-1
 SNDT is at level 1 Medium IoT-2, IoT-3, OT-1
 SNDT is at level 2 High WE-1, RO-1, MOB-1, PC-*, LA-*, PS-1, SE-*

4102 B.4.9 TH-PDOS: Denial of service attack on product functions via user or 4103 network access

4104 Attacker may use user or network access for a denial-of-service attack on product functions.

4105 Requirements that mitigate this threat: AUTH, LCKT, AVAI, LMII, LOGG, VULH

4106 Mitigations for Likelihood:

- 4107 • Medium to Low: RRDS
- 4108 • High to Low: RRDS, VULH

Risk factors	Likelihood	
none of NUSR, CUSR, or FNET is above level 0	Low	LR, IoT-1
the highest of NUSR, CUSR, and FNET is at level 1	Medium	IoT-2, IoT-3, OT-1, MOB-1, WE-1, PC-*, LA-*, SE-1, SE-2
any of NUSR, CUSR, or FNET is at level 2	High	RO-1, PS-1, SE-3

4109 Mitigations for Impact:

- 4110 • Medium to Low: LMEM, LOGG
- 4111 • High to Low: AUTH, AVNT, FDRP, LMEM, FAIR, LOGG

Risk factors	Impact	Security profiles
SENF is at level 0	Low	LR, IoT-1, IoT-2, WE-1
SENF is at level 1	Medium	IoT-3, PC-1, LA-1, PS-1
SENF is at level 2	High	RO-1, OT-1, MOB-1, PC-2, LA-2, SE-*

4112 B.4.10 TH-DDOS: Denial of service attack on other products via exploitation 4113 of vulnerabilities or unauthorized use of product functions

4114 Attacker may use the network to exploit vulnerabilities in the product to attack other products.

4115 *Guidance: Traffic amplification attacks and other misuses of product functions are considered vulnerabilities and/or*
 4116 *unauthorized use for the purpose of this threat.*

4117 Requirements that mitigate this threat: NKEV, SSDD, SDEF, MSAF, LMII, MINI, LMAS, LOGG

4118 All mitigations from TH-KEVU apply (using that requirement's risk formula), plus:

Risk factors	Likelihood	Security profiles
FNET is at level 0	Low	LR, IoT-1, WE-1
FNET is at level 1	Medium	IoT-2, IoT-3, OT-*, MOB-1, PC-*, LA-*
FNET is at level 2	High	RO-1, PS-1, SE-*

4119 Mitigations for Impact:

- 4120 • Medium to Low: (RRIS or MAMP)
- 4121 • High to Low: MNET, MAMP

Risk factors	Impact	Security profiles
TNET is at level 0	Low	LR, IoT-1
TNET is at level 1	Medium	IoT-2, IoT-3, OT-*, WE-1
TNET is at level 2	High	RO-1, MOB-1, PC-*, LA-*, PS-1, SE-*

4122 **B.4.11 TH-MQSE: Masquerading authorized server**

4123 Attacker may masquerade as an authorized server to get unauthorized access to product assets.

4124 Requirements that mitigate this threat: CDTX, ENTX, CRYP, IDTX, INTT, AUTH, LOGG

4125 Mitigations for Likelihood:

- 4126 • Medium to Low: AUTH, SUDC, CDTX, ENTX, CRYP, IDTX, INTT
- 4127 • High to Low: AUTH, SUDC, CDTX, ENTX, CRYP, IDTX, INTT

Risk factors	Impact	Security profiles
TNET is at level 0	Low	LR, IoT-1
TNET is at level 1	Medium	IoT-2, IoT-3, OT-1, WE-1
TNET is at level 2	High	RO-1, MOB-1, PC-*, LA-*, PS-1, SE-*

4128 Mitigations for Impact:

- 4129 • Medium to Low: LOGG
- 4130 • High to Low: LOGG

Risk factors	Impact	Security profiles
none of SNDS, SNDT, or SENF is above level 0	Low	LR, IoT-1
the highest of SNDS, SNDT, and SENF is at level 1	Medium	IoT-2, IoT-3
any of SNDS, SNDT, or SENF is at level 2	High	RO-1, OT-1, MOB-1, WE-1, PC-*, LA-*, PS-1, SE-*

4131 **B.4.12 TH-LEAK: Data leak through side channels**

4132 Attacker may use the ability to run arbitrary software on the product to get unauthorized read access to confidential data.

4134 Requirements that mitigate this threat: MISO, DMIN, VULH

4135 Mitigations for Likelihood:

- 4136 • Medium to Low: VULH
- 4137 • High to Low: (RRMD or PMSC), VULH

Risk factors	Likelihood	Security profiles
CUSR is at level 0 or none of SNDS or SNDT is above level 0	Low	LR, IoT-*, RO-1, OT-1, WE-1
all others	Medium	SE-1, PC-*, LA-*
CUSR is at level 2 and any of SNDS or SNDT is at level 2	High	PS-1, SE-2, SE-3

4138 Mitigations for Impact:

- 4139 • Medium to Low: DMIN
- 4140 • High to Low: DMIN

Risk factors	Impact	Security profiles
none of SNDS or SNDT is above level 0	Low	LR, IoT-1
the highest of SNDS and SNDT is at level 1	Medium	IoT-2, IoT-3, WE-1
any of SNDS or SNDT is at level 2	High	RO-1, OT-1, MOB-1, PC-*, LA-*, PS-1, SE-*

4141 **B.4.13 TH-RDPS: Compromise of the remote data processing solution**
 4142 **boundary**

4143 Attacker may compromise the boundary between the product and a remote data processing solution by impersonating
 4144 the remote endpoint, or by disrupting availability of interactions exchanged across the boundary, affecting the
 4145 behaviour, state, configuration, or security of the RDPS-dependent product function described in clause 4.8.

4146 Requirements that mitigate this threat: RAUT, RTRY, CRYP, CDTX, ENTX, IDTX, INTT, LOGG

4147 Mitigations for Likelihood:

- 4148 • Medium to Low: RAUT, CRYP, CDTX, ENTX, IDTX, INTT

Risk factors	Likelihood	Security profiles
RDPS is at level 0	Not applicable	LR, IoT-1, RO-1, OT-1, MOB-1, PC-*, LA-*, PS-1, SE-*
RDPS is at level 1	Medium	IoT-2, IoT-3, WE-1

4149 Mitigations for Impact:

- 4150 • Medium to Low: RTRY, LOGG

Risk factors	Impact	Security profiles
RDPS is at level 0	Not applicable	LR, IoT-1, RO-1, OT-1, MOB-1, PC-*, LA-*, PS-1, SE-*
RDPS is at level 1	Medium	IoT-2, IoT-3, WE-1

4151 **B.5 Mapping of use cases to risk factors**

4152 NOTE: The “TOTAL” field is a consistency check to see if the risk factors sufficiently distinguish the differences
 4153 in risk tolerance between use cases.

Use case	N	C	D	P	S	S	S	P	U	L	H	S	D	T	F	C	A	S	R	TO
	U	U	A	P	N	N	E	H	EI	O	W	W	V	N	N	O	D	U	D	TA
	R	R	A	II	S	T	F	S	N	SS	M	D	C	E	E	N	M	P	P	L
U C- L R	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
U C- Io T- 1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	2
U C- Io T- 2	0	0	1	0	1	1	0	0	1	0	0	0	0	1	1	1	2	2	1	12
U C- Io	0	0	1	0	1	1	1	0	2	0	1	0	0	1	1	1	2	2	1	15

T-3																				
U C- R- O- 1	0	0	1	0	1	2	2	0	2	0	0	0	0	2	2	2	1	2	0	17
U C- O T- 1	0	0	0	0	1	1	2	2	1	0	0	0	0	1	1	2	1	2	0	14
U C- M O B- 1	1	1	2	2	2	2	2	2	2	2	0	2	2	2	1	2	2	2	0	31
U C- W E- 1	0	0	1	1	2	2	0	1	2	1	0	1	0	1	0	1	2	1	1	17
U C- P C- 1	1	1	2	1	2	2	1	0	2	0	2	2	1	2	1	2	2	2	0	26
U C- P C- 2	1	1	2	1	2	2	2	0	2	0	2	2	1	2	1	2	1	2	0	26
U C- L A- 1	1	1	2	1	2	2	1	1	2	1	1	2	2	2	1	2	2	2	0	28
U C- L A- 2	1	1	2	1	2	2	2	1	2	1	1	2	2	2	1	2	1	2	0	28
U C- PS -1	2	2	2	0	2	2	1	0	2	0	1	2	1	2	2	2	1	2	0	26
U C- S E- 1	1	1	2	0	2	2	2	0	2	0	1	2	1	2	1	2	0	2	0	23
U C- S	2	1	2	0	2	2	2	0	2	0	1	2	1	2	1	2	0	2	0	24

E-
2
U 2 2 2 0 2 2 2 0 2 0 1 2 1 2 2 2 0 2 0 26
C-
S
E-
3

4154 **B.6 Security profiles**

4155 **B.6.1 General**

4156 Each security profile is associated with a collection of risk factor levels. The security profiles are defined normatively in
4157 clause 5.3 where each profile lists the mitigations that a product conforming to that profile shall implement. This annex
4158 provides the risk-based rationale for how the security profiles were derived from the risk factors and threat assessments
4159 described in clauses B.2 through B.4.

4160 **B.6.2 Mapping of security profiles to risk factors**

4161 Security profiles are associated with sets of risk factor levels. Each security profile represents one or more use cases
4162 whose risks can be treated with the same set of mitigations.

Se c. Pr of.	N U S R	C U S R	D A T A	P P H S	S N D S	S N D T	S E N F	P H Y S	U E I N	L O SS	H W D	S W M D	D V C S	T N E T	F N E T	C O N F	A D M N	S U P P	R D P S	TO TA L
SP - L R	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SP - I o T- 1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	2
SP - I o T- 2	0	0	1	0	1	1	0	0	1	0	0	0	1	1	1	1	2	2	1	12
SP - I o T- 3	0	0	1	0	1	1	1	0	2	0	1	0	0	1	1	1	2	2	1	15
SP - R O- 1	0	0	1	0	1	2	2	0	2	0	0	0	0	2	2	2	1	2	0	17
SP - O T- 1	0	0	0	0	1	1	2	2	1	0	0	0	0	1	1	2	1	2	0	14

SP	1	1	2	2	2	2	2	2	2	2	0	2	2	2	1	2	2	2	0	31
-																				
M																				
O																				
B-																				
1																				
SP	0	0	1	1	2	2	0	1	2	1	0	1	0	1	0	1	2	1	1	17
-																				
W																				
E-																				
1																				
SP	1	1	2	1	2	2	1	0	2	0	2	2	1	2	1	2	2	2	0	26
-																				
P																				
C-																				
1																				
SP	1	1	2	1	2	2	2	0	2	0	2	2	1	2	1	2	1	2	0	26
-																				
P																				
C-																				
2																				
SP	1	1	2	1	2	2	1	1	2	1	1	2	2	2	1	2	2	2	0	28
-																				
L																				
A-																				
1																				
SP	1	1	2	1	2	2	2	1	2	1	1	2	2	2	1	2	1	2	0	28
-																				
L																				
A-																				
2																				
SP	2	2	2	0	2	2	1	0	2	0	1	2	1	2	2	2	1	2	0	26
-																				
PS																				
-1																				
SP	1	1	2	0	2	2	2	0	2	0	1	2	1	2	1	2	0	2	0	23
-																				
S																				
E-																				
1																				
SP	2	1	2	0	2	2	2	0	2	0	1	2	1	2	1	2	0	2	0	24
-																				
S																				
E-																				
2																				
SP	2	2	2	0	2	2	2	0	2	0	1	2	1	2	2	2	0	2	0	26
-																				
S																				
E-																				
3																				

4164 **Annex C (informative):**
4165 **Change history**

Date	Version	Information about changes
<Month year>	<#>	<Changes made are listed in this cell>

4166 **7.23 History**

Document History

Version	Date	Milestone
	<#>	

4167