



Cybersecurity (CYBER); Cyber Resilience Act (CRA); Cybersecurity requirements for routers, modems intended for the connection to the internet and switches

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 304 627 Routers modems and switches · 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-0013

Keywords

CRA; Cybersecurity; router, modem, switch

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 in any form or by any means except for the purpose of implementation of standards.

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 2026.
All rights reserved.

5	Contents		
6	Intellectual Property Rights		7
7	Foreword.....		8
8	Modal verbs terminology		9
9	Introduction		10
10	1 Scope.....		11
11	2 References.....		12
12	2.1 Normative references.....		12
13	2.2 Informative references		13
14	3 Definition of terms, symbols and abbreviations.....		15
15	3.1 Terms.....		15
16	3.2 Symbols		16
17	3.3 Abbreviations.....		16
18	4 Product context.....		18
19	4.1 Introduction.....		18
20	4.2 Product functions		18
21	4.2.1 General product functions		18
22	4.2.1.1 General		18
23	4.2.1.2 [FN-G-01] Configuration and management		18
24	4.2.1.3 [FN-G-02] Monitoring and diagnostics		18
25	4.2.1.4 [FN-G-03] Access control		18
26	4.2.2 Product functions implemented by routers and switches		18
27	4.2.2.1 General		18
28	4.2.2.2 [FN-RS-01] Topology discovery		18
29	4.2.2.3 [FN-RS-02] Handling of network traffic processing rules		18
30	4.2.2.4 [FN-RS-03] Traffic access control		19
31	4.2.3 Product functions implemented by routers.....		19
32	4.2.3.1 General		19
33	4.2.3.2 [FN-R-01] Routing		19
34	4.2.3.3 [FN-R-02] WAN connectivity		19
35	4.2.4 Product functions implemented by switches		19
36	4.2.4.1 General		19
37	4.2.4.2 [FN-S-01] Switching		19
38	4.2.5 Product functions implemented by modems intended for connection to the internet.....		19
39	4.2.5.1 General		19
40	4.2.5.2 [FN-M-01] WAN connectivity		19
41	4.2.5.3 [FN-M-02] ISP-side remote management		19
42	4.2.6 Additional product capabilities		19
43	4.3 Product architecture.....		20
44	4.3.1 Product assets.....		20
45	4.4 Operational environment		21
46	4.4.1 General description		21
47	4.4.1.1 General		21
48	4.4.1.2 Residential deployments.....		21
49	4.4.1.3 Small enterprise deployments.....		21
50	4.4.1.4 Medium enterprise deployments.....		21
51	4.4.1.5 Large enterprise deployments.....		22
52	4.4.1.5.1 General.....		22
53	4.4.1.5.2 Data centre deployments.....		22
54	4.4.1.5.3 Service provider and carrier networks		23
55	4.4.2 Physical environment		23
56	4.4.3 Logical environment		23
57	4.4.4 Connectivity aspects.....		23
58	4.5 Distribution of security functions		24
59	4.6 Users		24

60	4.6.1	General	24
61	4.6.2	Natural persons.....	24
62	4.6.3	Legal entities	24
63	4.6.4	Devices.....	25
64	4.7	Use cases.....	25
65	4.7.1	General	25
66	4.7.2	Basic use cases	25
67	4.7.2.1	Physical devices for non-professional use	25
68	4.7.2.2	Physical devices for professional use	25
69	4.7.2.3	Routers and switches provided as virtual network functions.....	25
70	4.7.3	Supplementary use cases	25
71	4.7.3.1	Internet-facing enterprise edge devices	25
72	4.7.3.2	Devices within critical infrastructure.....	25
73	4.7.3.3	Devices within service provider and carrier network infrastructure.....	26
74	4.7.3.4	Devices serving persons with special protection needs	26
75	5	Technical requirements for the products	27
76	5.1	Introduction - Applicability of the requirements	27
77	5.2	Appropriate level of cybersecurity.....	27
78	5.3	No known exploitable vulnerabilities	27
79	5.3.1	[KEV-1] No known exploitable vulnerabilities	27
80	5.3.1.1	General	27
81	5.3.1.2	Requirements	27
82	5.4	Secure by default configuration	27
83	5.4.1	[DEFAULT-1] Secure by default configuration	27
84	5.4.1.1	General	27
85	5.4.1.2	Requirements	28
86	5.4.2	[RESET-1] Factory reset.....	29
87	5.4.2.1	General	29
88	5.4.2.2	Requirements	29
89	5.5	Secure updates	29
90	5.5.1	[UPDATE-1] Update mechanisms	29
91	5.5.1.1	General	29
92	5.5.1.2	Requirements	29
93	5.6	Authentication and access control	30
94	5.6.1	[AUTH-1] Authentication.....	30
95	5.6.1.1	General	30
96	5.6.1.2	Requirements	30
97	5.6.2	[AUTH-2] Authorization.....	30
98	5.6.2.1	General	30
99	5.6.2.2	Requirements	30
100	5.6.3	[AUTH-3] Authenticated session lifecycle	31
101	5.6.3.1	General	31
102	5.6.3.2	Requirements	31
103	5.6.4	[AUTH-4] Protocol access control.....	31
104	5.6.4.1	General	31
105	5.6.4.2	Requirements	31
106	5.7	Data protection.....	32
107	5.7.1	General	32
108	5.7.2	Requirements.....	32
109	5.8	Availability and resilience	33
110	5.8.1	General	33
111	5.8.2	Requirements.....	33
112	5.9	Attack surface and mitigation	33
113	5.9.1	[INTEGRITY-1] System integrity and boot process.....	33
114	5.9.1.1	General	33
115	5.9.1.2	Requirements	33
116	5.9.2	[PACKET-1] Default packet disposition.....	34
117	5.9.2.1	General	34
118	5.9.2.2	Requirements	34
119	5.9.3	[EXPOSURE-1] Interface and service exposure minimization.....	34
120	5.9.3.1	General	34

121	5.9.3.2	Requirements	34
122	5.10	Monitoring and logging	35
123	5.10.1	General	35
124	5.10.2	Requirements.....	35
125	5.11	Data management	35
126	5.11.1	[TRANSFER-1] Secure data export and transfer	35
127	5.11.1.1	General	35
128	5.11.1.2	Requirements	35
129	6	Assessment criteria for compliance with technical requirements	36
130	6.1	Introduction to the assessment and compliance criteria.....	36
131	6.2	No known exploitable vulnerabilities	36
132	6.2.1	[KEV-1] No known exploitable vulnerabilities	36
133	6.2.1.1	Requirement assessments	36
134	6.3	Secure by default configuration	38
135	6.3.1	[DEFAULT-1] Secure by default configuration	38
136	6.3.1.1	Requirement assessments	38
137	6.3.2	[RESET-1] Factory reset.....	49
138	6.3.2.1	Requirement assessments	49
139	6.4	Security updates.....	51
140	6.4.1	[UPDATE-1] Update mechanisms	51
141	6.4.1.1	Requirement assessments	51
142	6.5	Access control.....	57
143	6.5.1	[AUTH-1] Authentication	57
144	6.5.1.1	Requirement assessments	57
145	6.5.2	[AUTH-2] Authorization.....	64
146	6.5.2.1	Requirement assessments	64
147	6.5.3	[AUTH-3] Authenticated session lifecycle	67
148	6.5.3.1	Requirement assessments	67
149	6.5.4	[AUTH-4] Protocol access control.....	72
150	6.5.4.1	Requirement assessments	72
151	6.6	Data protection.....	76
152	6.6.1	Requirement assessments	76
153	6.7	Availability and resilience	81
154	6.7.1	Requirement assessments	81
155	6.8	Attack surface and mitigation	85
156	6.8.1	[INTEGRITY-1] System integrity and boot process.....	85
157	6.8.1.1	Requirement assessments	85
158	6.8.2	[PACKET-1] Default packet disposition.....	89
159	6.8.2.1	Requirement assessments	89
160	6.8.3	[EXPOSURE-1] Interface and service exposure minimization.....	91
161	6.8.3.1	Requirement assessments	91
162	6.9	Monitoring and logging	92
163	6.9.1	Requirement assessments	92
164	6.10	Data management	95
165	6.10.1	[TRANSFER-1] Secure data export and transfer	95
166	6.10.1.1	Requirement assessments	95
167	Annex A (informative): Relationship between the present document and the requirements of		
168	EU Regulation (EU) 2024/2847 - the Cyber Resilience Act.....		99
169	Annex B (informative): Security analysis		101
170	B.1	General.....	101
171	B.2	Threat landscape	101
172	B.2.1	Threats related to vulnerability handling.....	101
173	B.2.2	Threats related to packet processing and availability of services.....	102
174	B.2.3	Threats related to access control and authentication	104
175	B.2.4	Threats related to tampering and data processing	104
176	B.3	Threat assessment framework	106
177	B.3.1	Introduction.....	106
178	B.3.2	Risk factors	107
179	B.3.2.1	Baseline risk factors	107
180	B.3.2.2	Management risk factors	107

181	B.3.2.3 Protocol implementation risk factors	108
182	B.3.2.4 Data operations risk factors.....	108
183	B.3.3 Threat justification and mitigation	109
184	Annex K (normative): Vertical specific state of the art cryptography	113
185	K.1 General.....	113
186	K.1.1 Classification of cryptographic algorithms as CRY-SOTA	113
187	K.2 Assessment criteria for compliance with cryptographic requirements.....	114
188	K.2.1 Assessment objective	114
189	K.2.2 Assessment preparation	114
190	K.2.3 Assessment activities	114
191	K.2.4 Assessment evidence	114
192	K.2.5 Assessment verdict	115
193	K.3 Symmetric atomic primitives.....	116
194	K.3.1 Block ciphers	116
195	K.3.2 Stream ciphers.....	116
196	K.3.3 Hash functions	116
197	K.4 Symmetric constructions.....	116
198	K.4.1 Confidentiality modes of operation: encryption/decryption modes	116
199	K.4.2 Specific confidentiality modes: disk encryption	117
200	K.4.3 Integrity modes: message authentication codes	117
201	K.4.4 Symmetric entity authentication schemes	117
202	K.4.5 Authenticated encryption	117
203	K.4.6 Key protection.....	117
204	K.4.7 Key derivation functions.....	117
205	K.4.8 Password protection/password hashing mechanisms.....	117
206	K.4.9 Key combiners	118
207	K.5 Asymmetric atomic primitives.....	118
208	K.5.1 RSA/Integer factorization	118
209	K.5.2 Discrete logarithm in finite fields	118
210	K.5.3 Discrete logarithm in elliptic curves	118
211	K.5.4 Learning with errors in (structured) lattices.....	118
212	K.5.5 Hash function preimage resistance	118
213	K.5.6 Other intractable problems.....	119
214	K.6 Asymmetric constructions	119
215	K.6.1 Asymmetric encryption scheme.....	119
216	K.6.2 Digital signature.....	119
217	K.6.3 Asymmetric entity authentication schemes.....	119
218	K.6.4 Key establishment and key encapsulation.....	119
219	K.7 Cryptographic protocols.....	120
220	K.7.1 QUIC 120	
221	K.7.2 MACSec	120
222	K.7.3 SNMP 120	
223	K.7.4 Routing protocols.....	120
224	K.7.5 Secure device identity	121
225	K.7.6 Time Protocols.....	121
226	K.8 Cryptographic industry standards	122
227	K.9 Crypto agility	122
228	K.9.1 Requirement.....	122
229	K.9.2 Assessment of crypto-agility.....	123
230	K.9.2.1 Assessment objective	123
231	K.9.2.2 Assessment preparation	123
232	K.9.2.3 Assessment activities	123
233	K.9.2.4 Assessment evidence	123
234	K.9.2.5 Assessment verdict.....	124
235		
236		
237		

238

Intellectual Property Rights

239

Essential patents

240

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

241

242

243

244

245

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

246

247

248

249

Trademarks

250

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

251

252

253

254

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

255

256

257

258

259

Foreword

260
261
262

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

263
264
265
266
267

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

268
269
270
271

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

Proposed national transposition dates

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

272

273 **Modal verbs terminology**

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

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

278

279

Introduction

280

The present document covers cybersecurity for routers, modems intended for connection to the internet, and switches.

281

These products are identified in Annex III, Class I, point 12 of Regulation (EU) 2024/2847 [i.1], known as the Cyber

282

Resilience Act (CRA).

283

The present document provides a structured approach to identify the applicable cybersecurity requirements for the

284

products in scope, following a risk-based approach. Security controls are therefore proportionate to the intended

285

purpose, reasonably foreseeable use, deployment context, and threat exposure of the products.

286

Clause 4 describes the product architecture and intended purpose, and defines the use cases for the main deployment

287

scenarios under reasonably foreseeable use.

288

Clause 5 specifies the technical cybersecurity requirements for the product to mitigate the identified risks.

289

Clause 6 specifies the assessment criteria and compliance verification procedures for the requirements of clause 5.

290

Annex A maps the technical requirements of the present document to the corresponding cybersecurity requirements of

291

the CRA [i.1].

292

Annex B describes the methodology used to assess the security risks of the products in their context. Where a product

293

does not clearly correspond to one of the use cases defined in clause 4, the risk assessment methodology of Annex B

294

may be used to determine the applicable cybersecurity requirements.

295

296

1 Scope

297

298

299

The present document specifies vulnerability handling activities, technical requirements and corresponding assessment criteria for routers, modems intended for connection to the internet, and switches related to cybersecurity. The products with digital elements in scope:

300

301

302

303

- are specified within the "technical description" of the "category of product" in Class I, point 12 by the Commission Implementing Regulation (EU) 2025/2392 [i.2] of 28 November 2025 on the technical description of the categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of the Council [i.1] as:

304

305

306

- "Routers are products with digital elements that establish and control the flow of data between different networks by selecting paths or routes using routing protocol mechanisms and algorithms, typically operating at the network layer.

307

308

This category includes but is not limited to wired and wireless routers, virtual routers and routers with or without modems.";

309

310

311

- "Modems intended for the connection to the Internet are hardware products with digital elements that use digital modulation and demodulation techniques to convert analogue signals from and to digital signals for IP-based communication.

312

313

This category includes but is not limited to fibre modems, Digital Subscriber Line (DSL) modems, cable (DOCSIS) modems, satellite modems and cellular modems.";

314

315

- "Switches are products with digital elements that provide connectivity between networked devices through traffic forwarding mechanisms typically implemented at the data link layer.

316

317

318

This category includes but is not limited to managed switches, smart switches, multilayer switches, virtual security switches, programmable switches for software-defined networking and bridges such as wireless access points.";

319

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

320

321

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

322

323

324

NOTE 1: The term "internet" refers to any public network accessible beyond organizational boundaries. Public networks are accessible to multiple organizations or the general public. Private networks operate under single organizational control.

325

326

327

328

329

Routers, modems intended for connection to the internet, and switches fall within the scope of the present document when they provide management capabilities. This applies to all deployment forms such as dedicated hardware, virtual machines, containerized applications, and cloud-native network functions. The intended purpose or reasonably foreseeable use is to process, forward, or manage network traffic between devices, network segments, or between public and private networks.

330

331

NOTE 2: Unmanaged products with fixed functionality and no configuration interface are excluded from scope, as they lack the interfaces needed to implement the security controls of the present document.

332

333

334

The present document does not specify protocol conformance requirements, performance specifications, QoS metrics, or interoperability testing. Security controls for protocol implementation and vulnerability management remain within scope.

335

336

337

NOTE 3: Products that integrate particular wireless or wired communication technologies, such as Wi-Fi®, cellular, DECT, and DECT-2020 NR remain within scope when they function as routers, modems intended for connection to the internet, or switches

338

The present document is applicable to routers, modems intended for the connection to the internet and switches.

339

340

Routers, modems intended for connection to the internet, and switches intended for use in the industrial OT (Operational Technology) domain are excluded from the scope of the present document, see prEN 50770-5 [i.13].

341

342 2 References

343 2.1 Normative references

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

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

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

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

352 [1] prEN 40000-1-1: "Cybersecurity requirements for products with digital elements - Vocabulary",
353 (produced by CEN/CENELEC).

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

355 [2] prEN 40000-1-2: "Cybersecurity requirements for products with digital elements - Part 1-2:
356 Principles for cyber resilience", (produced by CEN/CENELEC).

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

358 [3] prEN 40000-1-3: "Cybersecurity requirements for products with digital elements - Part 1-3:
359 Vulnerability Handling", (produced by CEN/CENELEC).

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

361 [4] European Cybersecurity Certification Group, Sub-group on Cryptography: "Agreed Cryptographic
362 Mechanisms", Version 2.0, April 2025.

363 [5] BSI TR-02102-1 (Version 2026-01, 31 January 2026): "Cryptographic Mechanisms:
364 Recommendations and Key Lengths", <https://www.bsi.bund.de/dok/TR-02102-en>.

365 [6] ANSSI Référentiel Général de Sécurité, Annex B2: "Choice and Sizing of Cryptographic
366 Mechanisms".

367 [7] Canadian Centre for Cyber Security ITSP.40.062: "Guidance on Securely Configuring Network
368 Protocols".

369 [8] NIST SP 800-131A Rev. 2 (March 2019): "Transitioning the Use of Cryptographic Algorithms
370 and Key Lengths".

371 [9] ETSI TS 119 312: "Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites".

372 [10] ETSI TS 133 210: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal
373 Mobile Telecommunications System (UMTS); LTE; 5G; Network Domain Security (NDS); IP
374 network layer security".

375 [11] IETF RFC 8439: "ChaCha20 and Poly1305 for IETF Protocols".

376 [12] IETF RFC 4418: "UMAC: Message Authentication Code using Universal Hashing".

377 [13] IEEE 802.11-2020: "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY)
378 Specifications".

379 [14] IETF RFC 9106: "Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work
380 Applications".

381 [15] IETF RFC 7914: "The scrypt Password-Based Key Derivation Function".

382 [16] IETF RFC 5295: "Specification for the Derivation of Root Keys from an Extended Master Session
383 Key (EMSK)".

- 384 [17] IETF RFC 8410: "Algorithm Identifiers for Ed25519, Ed448, X25519, and X448 for Use in the
385 Internet X.509 Public Key Infrastructure".
- 386 [18] IETF RFC 8032: "Edwards-Curve Digital Signature Algorithm (EdDSA)".
- 387 [19] IETF RFC 8420: "Using the Edwards-Curve Digital Signature Algorithm (EdDSA) in the Internet
388 Key Exchange Protocol Version 2 (IKEv2)".
- 389 [20] IETF RFC 8110: "Opportunistic Wireless Encryption".
- 390 [21] Wi-Fi Alliance: "Easy Connect Specification", version 3.0.
- 391 [22] IETF RFC 9000: "QUIC: A UDP-Based Multiplexed and Secure Transport".
- 392 [23] IEEE 802.1AE-2018: "IEEE Standard for Local and Metropolitan Area Networks - Media Access
393 Control (MAC) Security".
- 394 [24] IETF RFC 3411: "An Architecture for Describing Simple Network Management Protocol (SNMP)
395 Management Frameworks".
- 396 [25] IETF RFC 3412: "Message Processing and Dispatching for the Simple Network Management
397 Protocol (SNMP)".
- 398 [26] IETF RFC 8205: "BGPsec Protocol Specification".
- 399 [27] IETF RFC 5709: "OSPFv2 HMAC-SHA Cryptographic Authentication".
- 400 [28] IETF RFC 7166: "Supporting Authentication Trailer for OSPFv3".
- 401 [29] IETF RFC 5310: "IS-IS Generic Cryptographic Authentication".
- 402 [30] IETF RFC 5925: "The TCP Authentication Option".
- 403 [31] IEEE 802.1AR-2018: "IEEE Standard for Local and Metropolitan Area Networks - Secure Device
404 Identity".
- 405 [32] IEEE 1588-2019: "IEEE Standard for a Precision Clock Synchronization Protocol for Networked
406 Measurement and Control Systems".
- 407 [33] IETF RFC 8915: "Network Time Security for the Network Time Protocol".
- 408 [34] BSI TR-02102-2 (Version 2026-01): "Cryptographic Mechanisms: Recommendations and Key
409 Lengths - Use of Transport Layer Security (TLS)", <https://www.bsi.bund.de/dok/TR-02102-en>.
- 410 [35] BSI TR-02102-3 (Version 2026-01): "Cryptographic Mechanisms: Recommendations and Key
411 Lengths - Use of Internet Protocol Security (IPsec) and Internet Key Exchange (IKEv2)",
412 <https://www.bsi.bund.de/dok/TR-02102-en>.
- 413 [36] BSI TR-02102-4 (Version 2026-01): "Cryptographic Mechanisms: Recommendations and Key
414 Lengths - Use of Secure Shell (SSH)", <https://www.bsi.bund.de/dok/TR-02102-en>.

415 2.2 Informative references

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

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

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

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

- 427 [i.2] Commission Implementing Regulation (EU) 2025/2392 of 28 November 2025 on the technical
428 description of the categories of important and critical products with digital elements pursuant to
429 Regulation (EU) 2024/2847 of the European Parliament and of the Council.
- 430 [i.3] Standardisation request M/606 - C(2025)618: "Commission Implementing decision of 3.2.2025 on
431 a standardisation request to the European Committee for Standardisation (CEN), the European
432 Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications
433 Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU)
434 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal
435 cybersecurity requirements for products with digital elements and amending Regulations (EU) No
436 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)".
- 437 [i.4] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on
438 the resilience of critical entities and repealing Council Directive 2008/114/EC.
- 439 [i.5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the
440 protection of natural persons with regard to the processing of personal data and on the free
441 movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- 442 [i.6] Recommendation ITU-T Y.2011 (2004): "General principles and general reference model for Next
443 Generation Networks".
- 444 [i.7] IETF RFC 7426 (2015): "Software-Defined Networking (SDN): Layers and Architecture
445 Terminology".
- 446 [i.8] NIST SP 800-133 Rev. 2 (June 2020): "Recommendation for Cryptographic Key Generation".
- 447 [i.9] ISO/IEC/IEEE 24765:2017: "Systems and software engineering - Vocabulary".
- 448 [i.10] IEEE Std 802.11-2024: "IEEE Standard for Information Technology - Telecommunications and
449 Information Exchange between Systems Local and Metropolitan Area Networks - Specific
450 Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY)
451 Specifications".
- 452 [i.11] Broadband Forum TR-069 Issue 1 Amendment 6 Corrigendum 1 (June 2020): "CPE WAN
453 Management Protocol".
- 454 [i.12] Broadband Forum TR-369 Issue 1 Amendment 4 Corrigendum 1 (June 2025): "User Services
455 Platform (USP)".
- 456 [i.13] prEN 50770-5: "Security for Operational Technologies - Part 5: Security Profile for routers,
457 modems intended for the connection to the internet, and switches", (produced by
458 CEN/CENELEC).
- 459 NOTE: Version and date to be added upon its publication by CEN/CENELEC.
- 460 [i.14] ENISA European Vulnerability Database (EUVD), established pursuant to Article 12(2) of
461 Directive (EU) 2022/2555, <https://euvd.enisa.europa.eu/>.
- 462 [i.15] ENISA Single Reporting Platform (SRP) established for Regulation (EU) 2024/2847,
463 [https://www.enisa.europa.eu/topics/product-security-and-certification/single-reporting-platform-](https://www.enisa.europa.eu/topics/product-security-and-certification/single-reporting-platform-srp)
464 [srp](https://www.enisa.europa.eu/topics/product-security-and-certification/single-reporting-platform-srp).
- 465

466 3 Definition of terms, symbols and abbreviations

467 3.1 Terms

468 For the purposes of the present document, the terms given in Regulation (EU) 2024/2847 [i.1], prEN 40000-1-1 [1] and
469 the following apply:

470 **access point:** network function that provides a wireless local area network for other devices, allowing them to access
471 device services or connect to private or public networks

472 NOTE: Access points can use various wireless technologies. In home routers, this function is implemented using
473 IEEE 802.11 technologies.

474 **audit event:** timestamped, structured record of activities including authentication attempts, configuration changes, and
475 product errors

476 **critical security parameter:** confidential information whose disclosure or modification can compromise product
477 security

478 EXAMPLE: Secret cryptographic keys, authentication values such as passwords, PINs, private components of
479 certificates.

480 **cryptographic algorithm:** sequence of instructions based on mathematical properties to protect confidentiality,
481 integrity or authenticity against attacks

482 NOTE: Cryptographic algorithms describe cryptographic protocols/schemes/constructors/atomic primitives such
483 as TLS/Symmetric Entity Authentication Schemes/AES-128 as part of a CMAC/AES-256.

484 **diagnostic:** pertaining to the detection and isolation of faults or failures

485 NOTE: As defined in ISO/IEC/IEEE 24765 [i.9] clause 3.1190.

486 **diagnostic interface:** interface used for diagnostic or troubleshooting purposes, not part of the intended function of the
487 product

488 EXAMPLE: UART, JTAG, and SWD.

489 **factory reset:** mechanism that restores the product to product factory default state

490 **firmware:** software stored in non-volatile memory that controls product operation

491 NOTE 1: Firmware includes boot sequences, operating system components, network protocol implementations, and
492 management interfaces.

493 NOTE 2: Firmware can include persistent configuration data required for product operation.

494 **legacy protocol:** network protocol whose specification lacks state of the art cryptography to ensure the authenticity,
495 integrity or confidentiality of security-relevant exchanges, where a secure alternative protocol or profile is widely
496 available, and which is retained in the product exclusively to maintain interoperability with deployed systems

497 EXAMPLE: Protocols whose role is limited to local IP address configuration, local neighbour and address
498 discovery, and name and service resolution are not considered legacy protocols for the purposes of the
499 present document, irrespective of their cryptographic properties. These protocols are designed under
500 explicit assumptions that specific risks are managed by the operational environment in which they are
501 deployed, and are required for basic network attachment and reachability.

502 NOTE: A vulnerability in a specific implementation of a protocol does not, by itself, make the protocol a legacy
503 protocol. Vulnerabilities associated with a legacy protocol can originate in its specification, in a specific
504 implementation, or in both.

505 **legacy system:** system that operates using at least one legacy protocol

506 **network interface:** physical interface that can be used to access the functionality of router, modem intended for
507 connection to the internet, or switch via a network

508 **private network:** closed network within a home or an organization that is not directly accessible by the general public
509 and is controlled by or on behalf of the user

- 510 **product:** router, modem intended for connection to the internet, or switch within the scope of the present document
- 511 **product factory default state:** state of the product as provided after manufacturing, reflecting the default configuration
512 established by the manufacturer, to which the product returns after a factory reset
- 513 NOTE 1: Depending on the product design and business model, security functionalities, for example secure boot,
514 trust anchors, or security policies, can be enabled by the manufacturer prior to delivery, or activated and
515 configured by the customer or authorized operator during initial setup.
- 516 NOTE 2: The product can be delivered by the manufacturer to an importer or distributor that subsequently sells it to
517 customers or puts it into service. In that case additional steps, for example finalization of configuration,
518 can be required before the product enters an operational state.
- 519 **product operational state:** state in which the product can operate within its intended purpose and reasonably
520 foreseeable use with its current active configuration, whether this configuration corresponds to the preconfigured
521 default settings or has been modified by the user
- 522 **public network:** network that is accessible by the general public and is not controlled by a user
- 523 EXAMPLE: Mobile networks such as 5G, or the internet.
- 524 **reboot:** a specific management operation or autonomous reaction to product state that triggers a product restart
- 525 **secure channel:** path for transferring data between two entities or components that ensures confidentiality, integrity,
526 and replay protection, as well as mutual authentication between the entities or components
- 527 NOTE 1: The secure channel can be provided using cryptographic, physical, or procedural methods or a
528 combination thereof.
- 529 NOTE 2: SOURCE: NIST SP 800-133 Rev. 2 [i.8].
- 530 **secure-by-default configuration:** configuration in which the product satisfies requirements in clause [5.4.1](#)
- 531 **software bill of materials:** formally structured list of all software components, libraries, and dependencies included in
532 the product, with version identifiers
- 533 **Transport Layer Port:** a logical interface on OSI Layer 4 used to address applications on a host that take part in end-
534 to-end information exchange
- 535 NOTE: A host can run many network applications behind a single IP address. The Transport Layer Port Number
536 identifies each application separately.
- 537 **Wi-Fi® network:** wireless local area network implemented according to IEEE 802.11 [i.10]
- 538 NOTE: In residential environments, Wi-Fi® is commonly used as the primary method for devices to connect to
539 the public network and access the internet.

540 3.2 Symbols

541 Void.

542 3.3 Abbreviations

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

API	Application Programming Interface
ARP	Address Resolution Protocol
CRA	Cyber Resilience Act
DECT	Digital Enhanced Cordless Telecommunications
DECT-2020 NR	Digital Enhanced Cordless Telecommunications 2020 New Radio
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DSL	Digital Subscriber Line
EU	European Union
GDPR	General Data Protection Regulation
IDS	Intrusion Detection System

IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPR	Intellectual Property Rights
IPS	Intrusion Prevention System
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
JTAG	Joint Test Action Group
LAN	Local Area Network
LTE	Long Term Evolution
MAC	Media Access Control
NAT	Network Address Translation
OSI	Open Systems Interconnection
QoS	Quality of Service
RFC	Request for Comments
SBOM	Software Bill of Materials
SWD	Serial Wire Debug
UART	Universal Asynchronous Receiver-Transmitter
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VNF	Virtual Network Function
VPN	Virtual Private Network
WAN	Wide Area Network

544

545 4 Product context

546 4.1 Introduction

547 Routers are network infrastructure products that interconnect separate networks and direct traffic between them based
548 on OSI layer 3 addresses and routing policies. The present document covers consumer, enterprise, and virtual routers,
549 and those with integrated modem functions.

550 Modems intended for connection to the internet are network infrastructure products that connect to public networks by
551 converting signals between analogue and digital formats. The present document covers modems intended for connection
552 to the internet using wired, wireless, and cellular access technologies.

553 Switches are network infrastructure products that interconnect devices within a network by directing traffic based on
554 OSI layer 2 addresses. The present document covers managed, smart, multilayer, virtual, and programmable switches
555 and bridges such as wireless access points. Programmable variants may support software-defined networking
556 deployments.

557 4.2 Product functions

558 4.2.1 General product functions

559 4.2.1.1 General

560 The product functions in this clause apply to routers, modems intended for connection to the internet, and switches and
561 are not specific to any single product category.

562 4.2.1.2 [\[FN-G-01\]](#) Configuration and management

563 These functions provide management interfaces such as command-line, web-based, and API interfaces. They handle
564 network settings, traffic processing, security configurations, QoS rules, and maintenance tasks. They maintain
565 consistent settings across all components and block changes without authorization.

566 4.2.1.3 [\[FN-G-02\]](#) Monitoring and diagnostics

567 Monitoring functions collect interface statistics, error conditions, performance metrics, and security events. They
568 provide visibility into product operation and network traffic patterns. Diagnostics enable troubleshooting of
569 connectivity, performance, and configuration errors. Operational data is not exposed beyond the intended purpose.

570 4.2.1.4 [\[FN-G-03\]](#) Access control

571 The access control function regulates product access according to defined security policies. It determines which entities
572 or users may access and modify product configurations.

573 4.2.2 Product functions implemented by routers and switches

574 4.2.2.1 General

575 The product functions described in this clause apply to routers and switches only and are not applicable to modems
576 intended for connection to the internet.

577 4.2.2.2 [\[FN-RS-01\]](#) Topology discovery

578 Topology discovery describes the ability of products to identify at least partially the topology of connected networks at
579 the OSI layers the product operates at. This function covers capabilities such as neighbour discovery and MAC learning.

580 4.2.2.3 [\[FN-RS-02\]](#) Handling of network traffic processing rules

581 This function covers the ability of products to receive, derive, store, manipulate, and delete traffic processing rules at
582 the network layers the product operates at.

583 4.2.2.4 [\[FN-RS-03\]](#) Traffic access control

584 This function applies configured access control rules to network traffic, determining what traffic is permitted or
585 restricted.

586 4.2.3 Product functions implemented by routers

587 4.2.3.1 General

588 The product function described in this clause applies to routers only and is not applicable to switches or modems
589 intended for connection to the internet.

590 4.2.3.2 [\[FN-R-01\]](#) Routing

591 Routing describes the ability of routers to execute network traffic processing rules at OSI layer 3.

592 4.2.3.3 [\[FN-R-02\]](#) WAN connectivity

593 WAN connectivity describes the ability of routers to establish and maintain a physical link across a wide area network.

594 4.2.4 Product functions implemented by switches

595 4.2.4.1 General

596 The product function described in this clause applies to switches only and is not applicable to routers or modems
597 intended for connection to the internet.

598 4.2.4.2 [\[FN-S-01\]](#) Switching

599 Switching describes the ability of switches to execute network traffic processing rules at OSI layer 2.

600 4.2.5 Product functions implemented by modems intended for connection
601 to the internet

602 4.2.5.1 General

603 The product functions described in this clause apply to modems intended for connection to the internet only and are not
604 applicable to routers or switches.

605 4.2.5.2 [\[FN-M-01\]](#) WAN connectivity

606 WAN connectivity describes the ability of modems to establish and maintain a physical link across a wide area network.

607 4.2.5.3 [\[FN-M-02\]](#) ISP-side remote management

608 ISP-side remote management is the ability of modems to be configured and managed by a service provider. Broadband
609 Forum protocols such as TR-069 [\[i.11\]](#) and TR-369 [\[i.12\]](#) may be used for this purpose.

610 4.2.6 Additional product capabilities

611 In addition to the product functions above, the following non-exhaustive list of capabilities can be present:

- 612 [\[CAP-01\]](#) Integrated firewall capabilities
- 613 [\[CAP-02\]](#) VPN services
- 614 [\[CAP-03\]](#) Integrated Wireless Access Point
- 615 [\[CAP-04\]](#) Content filtering
- 616 [\[CAP-05\]](#) QoS management
- 617 [\[CAP-06\]](#) Network monitoring tools
- 618 [\[CAP-07\]](#) Network segmentation

- 619 [\[CAP-08\]](#) Virtualization or container execution stacks
- 620 [\[CAP-09\]](#) PKI Certification Authority functionality
- 621 [\[CAP-10\]](#) Network functions related to telecommunications

622 4.3 Product architecture

623 4.3.1 Product assets

624 Products implement a multi-plane architecture separating the data, control, and management planes as described in ITU-
625 T Y.2011 [\[i.6\]](#) and IETF RFC 7426 [\[i.7\]](#).

626 The data plane, also called the forwarding plane, implements only the functions in clauses [4.2.3.2](#) and [4.2.4.2](#). It can
627 employ the following assets, listed as non-exhaustive examples:

- 628 [\[AS-DP-01\]](#) Application-specific integrated circuits.
- 629 [\[AS-DP-02\]](#) Network processors optimized for packet processing operations
- 630 [\[AS-DP-03\]](#) Generalized central processing units

631 The control plane primarily implements the functions in clauses [4.2.2.2](#), [4.2.2.3](#), and [4.2.2.4](#). It can employ the
632 following assets, listed as non-exhaustive examples:

- 633 [\[AS-CP-01\]](#) MAC tables
- 634 [\[AS-CP-02\]](#) Routing tables
- 635 [\[AS-CP-03\]](#) Flow tables

636 The management plane provides interfaces for the functions in clauses [4.2.1.2](#), [4.2.1.3](#), and [4.2.1.4](#). It can employ the
637 following assets, listed as non-exhaustive examples:

- 638 [\[AS-MP-01\]](#) Command-line interfaces
- 639 [\[AS-MP-02\]](#) Web-based management consoles
- 640 [\[AS-MP-03\]](#) Programmatic APIs
- 641 [\[AS-MP-04\]](#) Management software
- 642 [\[AS-MP-05\]](#) Management plane protocol stacks

643 The physical architecture includes interfaces at different OSI layers, which are also product assets, listed as non-
644 exhaustive examples:

- 645 [\[AS-I-01\]](#) Ethernet interfaces per the IEEE 802.3 standards family
- 646 [\[AS-I-02\]](#) Wi-Fi® interfaces per IEEE 802.11
- 647 [\[AS-I-03\]](#) Fibre optic connectors
- 648 [\[AS-I-04\]](#) Console ports
- 649 [\[AS-I-05\]](#) USB interfaces
- 650 [\[AS-I-06\]](#) Out-of-band management interfaces

651 In addition to the plane-specific and interface-related assets, the following basic assets are also relevant:

- 652 [\[AS-B-01\]](#) Central processing units, primarily for control and management functions
- 653 [\[AS-B-02\]](#) Volatile memory
- 654 [\[AS-B-03\]](#) Non-volatile memory
- 655 [\[AS-B-04\]](#) Embedded operating system

656 [\[AS-B-05\]](#) Network protocol stacks

657 [\[AS-B-06\]](#) Encryption

658 4.4 Operational environment

659 4.4.1 General description

660 4.4.1.1 General

661 Products covered by the present document operate in diverse environments. Environments differ by applicable product
662 categories as described in clause [4.1](#), by the capabilities present as described in clause [4.2.6](#), and by the level of
663 virtualization. The operational context also matters. Relevant factors are network architecture, trust boundaries,
664 tolerance for downtime, level of configuration required after setup, user interaction, and traffic patterns.

665 Further criteria characterize the environments in the designated clauses. Physical protection levels are described in
666 clause [4.4.2](#). Logical protection levels are described in clause [4.4.3](#). Connectivity to entities in the same and adjacent
667 networks is described in clause [4.4.4](#).

668 4.4.1.2 Residential deployments

669 Residential deployments are characterized by the following properties:

- 670 • The deployed products are routers and modems intended for connection to the internet, which may be bundled
671 into one physical device.
- 672 • The deployed products are likely to incorporate wireless access points [\[CAP-03\]](#).
- 673 • The products are expected to operate with minimal technical oversight and to allow for plug-and-play
674 functionality with the given network environment.
- 675 • The network boundary between trusted products on the private network and the public network relies entirely
676 on the security controls these products implement, as additional security layers are seldom deployed in
677 residential environments.
- 678 • Traffic patterns are diverse, with examples such as streaming media, web browsing, remote work connections,
679 online gaming, and smart home device communications with cloud services.
- 680 • The product is likely to operate continuously, but occasional downtime may occur.

681 4.4.1.3 Small enterprise deployments

682 Small enterprise deployments such as small points of sale or offices of self-employed persons share many properties
683 with residential deployments as described in clause [4.4.1.2](#). The main differences from the residential deployment are
684 assumed to be the following:

- 685 • In addition to wireless access points [\[CAP-03\]](#), VPN services [\[CAP-02\]](#), content filtering [\[CAP-04\]](#), and basic
686 firewall capabilities [\[CAP-01\]](#) are more likely to be incorporated in the deployed product.
- 687 • Traffic patterns are driven mainly by business and can be as diverse as in residential deployments.
- 688 • The product is likely to operate continuously, but occasional downtime is considered tolerable and user
689 scheduled outside business hours. Administrators will likely be involved in monitoring and approving any
690 service impacting upgrades to the network infrastructure.

691 4.4.1.4 Medium enterprise deployments

692 Medium enterprises deploy network infrastructure for medium point-of-sale systems, employee workstations, guest
693 wireless networks, and connections to cloud-based business applications. These environments can be characterized as
694 follows:

- 695 • Products of all categories as defined in clause [4.1](#) are likely to be deployed. Modems intended for connection
696 to the internet, at minimum, are deployed as separate physical devices. Routers and switches may be deployed
697 as physical devices or virtual machines. The combination of routing functionality described in clause [4.2.3.2](#)
698 and switching functionality described in clause [4.2.4.2](#) within one device is permitted but not required.

- 699 • Typically, at least one of the deployed routers incorporates VPN services [\[CAP-02\]](#) to enable secure
700 connections for remote workers.
- 701 • At least some of the deployed routers are likely to incorporate wireless access points [\[CAP-03\]](#) for multiple
702 user groups such as guests and employees.
- 703 • The relevant or important products are expected to operate with technical oversight by the IT staff of the user
704 or a service provider. The products are therefore expected to enable management access by the IT staff or
705 service provider.
- 706 • Content filtering [\[CAP-04\]](#) and basic firewall capabilities [\[CAP-01\]](#) may be present where no dedicated
707 firewall is deployed at the network edge.
- 708 • Beyond basic internet connectivity, traffic patterns depend on the business.
- 709 • The products are likely to operate continuously, with low tolerance for downtime, though this varies by
710 business.

711 4.4.1.5 Large enterprise deployments

712 4.4.1.5.1 General

713 Large enterprises deploy network infrastructure for the same purposes as smaller enterprises but at a significantly larger
714 scale. These environments differ from those described in clause [4.4.1.4](#) as follows:

- 715 • High-performance products of all categories as defined in clause [4.1](#) are deployed. Multiple specialized
716 products are likely to be deployed within each category.
- 717 • Whether routers are deployed as virtual machines or as physical devices depends on the specific use. Modems
718 intended for connection to the internet and switches are deployed as separate physical devices to utilize
719 application-specific hardware.
- 720 • The network is likely to incorporate advanced network management and orchestration features.
- 721 • Downtime is not tolerated unless exceptionally scheduled and organized by the IT staff with management
722 access.
- 723 • Admin IT staff will be involved in approving and performing any upgrades to the network infrastructure.
- 724 • Routers, modems intended for connection to the internet, and switches in this environment are required to
725 support network monitoring [\[CAP-06\]](#), segmentation [\[CAP-07\]](#), and QoS management [\[CAP-05\]](#).
- 726 • Hierarchical network architectures with core, distribution, and access layers are likely to be used.
- 727 • Within the environment, dedicated security systems such as IDS/IPS, SIEM, or other defence systems are
728 deployed and specific incident response procedures are in place.
- 729 • The infrastructure supports diverse traffic types: real-time communications, database replication, backup
730 transfers, and user application traffic. Each type has specific performance and security requirements.
- 731 • Within the deployment, connections to adjacent networks including the internet are strictly restricted and
732 controlled by the environment's security systems.
- 733 • The size of such deployments requires a high level of automation across all operational aspects.

734 Large enterprises consider their IT normally as business critical, and these deployments can already belong to the
735 critical infrastructure. Therefore, the product deployment typically occurs only within a physically protected
736 environment providing strict access controls to the physical devices. The physical protection is typically shifted from
737 the product to the operational environment.

738 4.4.1.5.2 Data centre deployments

739 The traffic pattern is specific to large-scale data storage and service provision. The network topologies are optimized to
740 meet specific latency and redundancy requirements. The devices within this deployment are optimized for specific roles
741 within these topologies, such as leaf, spine, and top-of-rack switches within a leaf-spine architecture. Data centres may

742 serve an enterprise's own purposes or provide services to third parties. The latter can range from infrastructure as a
743 service to software as a service.

744 Admin IT staff will be involved in approving and performing any upgrades to the network infrastructure. These services
745 operate under service level agreements imposing strict requirements on the infrastructure's availability and reliability.

746 Data centre operators consider their IT normally as business critical and are typically subjected to GDPR [\[i.5\]](#) rules.
747 Also, these deployments can belong to the critical infrastructure. Therefore, the product deployment typically occurs
748 only within a physically protected environment providing strict access controls to the physical devices. The physical
749 protection is typically shifted from the product to the operational environment.

750 4.4.1.5.3 Service provider and carrier networks

751 Traffic patterns in this environment are diverse, spanning basic internet connectivity, voice and video calls, large
752 transfers, and business-specific communications. Network topology reflects both the architectural needs of
753 telecommunications systems and the geographic spread of customers. Products are specialized by task and location
754 within the network. IT staff will be involved in approving and performing any upgrades to the network infrastructure.

755 Network functions related to telecommunications [\[CAP-10\]](#) may be present.

756 Service providers and carriers consider their IT normally as business critical and the provided services are typically
757 critical for public services. Thus, these deployments belong to the critical infrastructure. Therefore, the product
758 deployment occurs only within a physically protected environment providing strict access controls to the physical
759 devices. The physical protection is typically shifted from the product to the operational environment.

760 4.4.2 Physical environment

761 In all environments described in clause [4.4.1](#), products are likely to operate in a physical environment accessible to a
762 limited number of persons. The main exception is products with wireless access points [\[CAP-03\]](#) serving publicly
763 accessible areas of an enterprise site. Physical protection ranges from the low level of private flats as described in clause
764 [4.4.1.2](#) and small enterprise offices as described in clause [4.4.1.3](#) to the high level of data centres as described in clause
765 [4.4.1.5.2](#), which occupy designated and physically protected sites and buildings.

766 4.4.3 Logical environment

767 In residential and small enterprise deployments as described in clauses [4.4.1.2](#) and [4.4.1.3](#), logical access is controlled
768 mainly by the products themselves. Security measures such as network boundary protection or centralized management
769 are seldom deployed. Network abstraction such as VLANs is uncommon, as non-technical users as described in clause
770 [4.6.2](#) are responsible for all manual changes to device configuration.

771 In medium to large enterprises, provider networks as described in clause [4.4.1.5.3](#), and data centres as described in
772 clause [4.4.1.5.2](#), network abstraction and virtualization are used to shape the logical environment. This enables specific
773 topologies such as leaf-spine or partial meshes, limiting the logical links of routers and switches.

774 4.4.4 Connectivity aspects

775 Within the residential environment described in clause [4.4.1.2](#), the products are connected to multiple devices of various
776 kinds such as personal computers, smartphones, smart home appliances, and entertainment systems. In small enterprises
777 as described in clause [4.4.1.3](#), the devices to which the products covered by the present document are connected are
778 likely to be less diverse and consist primarily of personal computers and smartphones. Modems intended for connection
779 to the internet within these two environments connect directly to internet service providers through cable, DSL, or fibre
780 connections.

781 In medium and large enterprise environments as described in clauses [4.4.1.4](#) and [4.4.1.5](#), respectively, the network
782 boundary between trusted products in the private network and the public network is likely to be protected by additional
783 security layers. These layers are provided by separate firewalls and security systems or incorporated as corresponding
784 capabilities on the routers. All products within the private network are logically connected to each other and the edge
785 devices of the aforementioned security layer, with network segmentation used to isolate virtual networks and prevent
786 lateral movements by adversaries. Only the edge devices need to be connected to the public network. This also holds for
787 data centre deployments as described in clause [4.4.1.5.2](#) and service provider and carrier networks as described in
788 clause [4.4.1.5.3](#).

789 4.5 Distribution of security functions

790 Security functions of routers, modems intended for connection to the internet, and switches relate to the assets and
791 capabilities described in clause [4.3](#). The security function deployment can be categorized as follows:

- 792 • Integration of security functions. In this case, the security functions rely on assets of the products that are
793 provided by third parties. This is likely to apply to assets such as integrated circuits [\[AS-DP-01\]](#), processors
794 [\[AS-DP-02\]](#) and [\[AS-B-01\]](#), memory [\[AS-B-02\]](#) and [\[AS-B-03\]](#), and cryptographic implementations [\[AS-B-](#)
795 [06\]](#) and silicon to support additional capabilities such as integrated wireless access points [\[CAP-03\]](#). The
796 present document addresses such security functions through integration requirements.
- 797 • Product-intrinsic deployment of security functions. In this case, the security functions rely on assets that are
798 likely to be part of the product design process itself such as MAC [\[AS-CP-01\]](#) or routing tables [\[AS-CP-02\]](#)
799 and capabilities such as integrated firewalls [\[CAP-01\]](#) or network segmentation [\[CAP-07\]](#). The present
800 document addresses such security functions through requirements directly applicable to the products.

801 Security functions of routers, modems intended for connection to the internet, and switches can be associated with the
802 assets and capabilities described in clause [4.3](#).

803 4.6 Users

804 4.6.1 General

805 The products are used by natural persons, legal entities, and other devices. Devices may include servers, computers, and
806 other network enabled equipment.

807 4.6.2 Natural persons

808 Natural persons can be grouped based on their technical expertise and level of responsibility. The following groups of
809 users may be present depending on the operational environment:

- 810 • Professional network administrators configure and maintain such products in corporate environments. They
811 analyse logs, respond to incidents, and automate product operation. They may be employed by the operating
812 legal entity or by a contractor. Their interaction with products is expected in medium to large enterprise and
813 service provider and carrier deployments as described in clauses [4.4.1.4](#), [4.4.1.5](#), and [4.4.1.5.3](#).
- 814 • Users and laymen without technical knowledge or experience have full legal capacity but no specific
815 knowledge of the products. Their interaction with products is expected in residential and small enterprise
816 deployments as described in clauses [4.4.1.2](#) and [4.4.1.3](#).
- 817 • Service provider personnel are qualified to carry out standard installation and maintenance of customer
818 premises equipment. They provide support to such users in residential and small enterprise deployments as
819 described in clauses [4.4.1.2](#) and [4.4.1.3](#).
- 820 • Users with special protection needs, which originate from their prominence, visibility or function in public life,
821 require additional protection means for their data handled by the products. Their interaction with products is
822 expected primarily in residential deployments as described in clause [4.4.1.2](#) but also in small and medium
823 enterprise deployments as described in clauses [4.4.1.3](#) and [4.4.1.4](#) that serve this user category. This category
824 includes, but is not limited to, children, heads of diplomatic delegations, and persons in commercial or
825 institutional roles requiring confidentiality. Enterprise deployments serving this category include schools, other
826 educational and childcare facilities, and diplomatic or governmental institutions.

827 4.6.3 Legal entities

828 Legal entities operate products in enterprise deployments as described in clauses [4.4.1.3](#), [4.4.1.4](#), and [4.4.1.5](#). They may
829 also operate products as a service to natural persons, making them relevant to residential deployments as described in
830 clause [4.4.1.2](#). They are categorized by their importance to the public as follows:

- 831 • Operators of critical infrastructure are of special importance to the public. A disruption of their operation can
832 have a severe impact on society.
- 833 • Legal entities without special legal obligation are those entities that are not operators of critical infrastructure.

834 4.6.4 Devices

835 Servers, computers, and other network enabled devices communicate on behalf of users or IT staff via the products
836 covered by the present document. Their interaction with the products is preconfigured and does not require direct
837 human intervention during normal operation. Their presence is expected in all deployment environments described in
838 clause [4.4.1](#).

839 4.7 Use cases

840 4.7.1 General

841 This clause identifies use cases for routers, modems intended for connection to the internet, and switches. The use cases
842 presented are neither exhaustive nor mutually exclusive. A single product can support multiple use cases, and the list
843 may be extended in future revisions. This clause considers two categories of use cases:

- 844 • Basic use cases describe reasonably foreseeable use of the product.
- 845 • Supplementary use cases derive from one or more basic use cases and introduce specific properties that add
846 risk factors.

847 For both categories, this clause describes only those characteristics considered relevant for subsequent threat
848 identification. Characteristics include the user categories and their properties as described in clause [4.6](#), as well as the
849 operational environments and their properties as described in clause [4.4](#).

850 4.7.2 Basic use cases

851 4.7.2.1 Physical devices for non-professional use

852 This use case covers residential and small enterprise deployments as described in clauses [4.4.1.2](#) and [4.4.1.3](#) where non-
853 technical users as described in clause [4.6.2](#) operate routers, modems intended for connection to the internet, or
854 combined devices. Products shall provide all required security functions by themselves. Where user interaction is
855 required, the product shall provide guidance and information to enable the user to complete the interaction.

856 4.7.2.2 Physical devices for professional use

857 This use case covers medium to large enterprise deployments as described in clauses [4.4.1.4](#) and [4.4.1.5](#) where
858 professional network administrators as described in clause [4.6.2](#) operate the products. The IT staff of the enterprise
859 configures and monitors product operations. Products in this use case have specialized capabilities, are optimized for
860 specific tasks, and operate under strict security controls. These controls may be provided by dedicated devices such as
861 firewalls, IDS, or IPS, or as capabilities of the products themselves.

862 4.7.2.3 Routers and switches provided as virtual network functions

863 This use case covers primarily medium to large enterprise deployments as described in clauses [4.4.1.4](#) and [4.4.1.5](#)
864 where routers and switches are deployed as VNF within a virtualization environment. The products as well as their
865 virtualization environment are operated by professional network administrators as described in clause [4.6.2](#). The VNF
866 are highly standardized allowing rapid and automated deployment and configuration. At least some of the security
867 controls need to be provided by the virtualization environment.

868 4.7.3 Supplementary use cases

869 4.7.3.1 Internet-facing enterprise edge devices

870 Within the basic use cases described in clauses [4.7.2.2](#) and [4.7.2.3](#), devices at network boundaries connecting private
871 networks to internet service providers or business partners are exposed to a significantly larger variety of threats. The
872 probability of these threats exceeds the commonly assumed majority of the basic use cases.

873 4.7.3.2 Devices within critical infrastructure

874 Within the basic use cases in clauses [4.7.2.2](#) and [4.7.2.3](#), devices in critical infrastructure face a wider range of threats at
875 higher probability than the average for those use cases. Such an enterprise is an operator of critical infrastructure as
876 described in clause [4.6.3](#). Operators provide a protected operational environment with strict physical and logical access

877 controls. They are subject to obligations from other regulations such as Directive (EU) 2022/2557 [\[i.4\]](#) on the resilience
878 of critical entities.

879 4.7.3.3 Devices within service provider and carrier network infrastructure

880 Within the basic use cases described in clauses [4.7.2.2](#) and [4.7.2.3](#), the devices can be deployed in the operational
881 environment of service provider and carrier networks as described in clause [4.4.1.5.3](#). The specific topology and spatial
882 extent of these networks give rise to specific threats. Operators provide a protected operational environment with strict
883 physical and logical access controls. They are subject to obligations from other regulations such as Directive (EU)
884 2022/2557 [\[i.4\]](#) on the resilience of critical entities. This supplementary use case requires consideration in addition to
885 the one described in clause [4.7.3.2](#).

886 4.7.3.4 Devices serving persons with special protection needs

887 When routers, modems intended for connection to the internet, and switches provide network connections for persons
888 with special protection needs as described in clause [4.6.2](#), additional threats apply. This use case primarily supplements
889 the basic use case described in clause [4.7.2.1](#) but can also supplement the use cases in clauses [4.7.2.2](#) and [4.7.2.3](#) when
890 the enterprise serves this user group.

891

892 5 Technical requirements for the products

893 5.1 Introduction - Applicability of the requirements

894 The technical requirements of the present document apply under the product context described in clause 4, which shall
895 be in accordance with its intended use. The product shall comply with all applicable technical requirements of the
896 present document at all times when operating in such product context.

897 Not all requirements are universally applicable. The applicability of requirements may be based on use cases or specific
898 capabilities of the product.

899 5.2 Appropriate level of cybersecurity

900 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (1).

901 The present document provides an appropriate level of cybersecurity based on the risks by:

- 902 • describing in clause 4 the product context, including the product functions, architecture, operational
903 environments, users, and use cases;
- 904 • describing in Annex B the threats associated with that product context and the risk factors that affect their
905 applicability and likelihood; and
- 906 • conditioning the applicability of the technical requirements in the subsequent subclauses on those use cases
907 and risk factors, so that the security controls required of a product are proportionate to the risks arising from its
908 intended purpose, reasonably foreseeable use, deployment context, and threat exposure.

909 The security controls required by the applicable technical requirements of the present document shall be integrated into
910 the product such that no security property required by one control is bypassed or weakened by the implementation or
911 operation of another control or product function.

912 5.3 No known exploitable vulnerabilities

913 5.3.1 [KEV-1] No known exploitable vulnerabilities

914 5.3.1.1 General

915 Products made available on the market are free of known exploitable vulnerabilities. The manufacturer maintains a
916 software bill of materials covering all product components and third-party dependencies. The assessor verifies the
917 software bill of materials against known vulnerability databases.

918 5.3.1.2 Requirements

919 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (a).

920 [\[REQ-KEV-1-01\]](#) The manufacturer shall maintain a software bill of materials for each product version in a machine-
921 readable format.

922 [\[REQ-KEV-1-02\]](#) The product shall contain no known exploitable vulnerabilities in each product version when made
923 available on the market.

924 [\[REQ-KEV-1-03\]](#) The manufacturer shall verify that third-party components in the product do not contain known
925 exploitable vulnerabilities before making each product version available on the market.

926 5.4 Secure by default configuration

927 5.4.1 [DEFAULT-1] Secure by default configuration

928 5.4.1.1 General

929 Products include security controls that are configured and enabled from initial deployment. This protects against
930 exploitation attempts that can occur within minutes of network connection. The default configuration establishes the

931 security baseline. Many users, particularly in residential and small business deployments, are expected to operate with
932 this configuration unchanged throughout the product lifecycle.

933 5.4.1.2 Requirements

934 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (b).

935 The requirements [\[REQ-DEFAULT-1-09\]](#), [\[REQ-DEFAULT-1-10\]](#) and [\[REQ-DEFAULT-1-11\]](#) apply, at the protocol
936 layer, the legacy-interoperability framework set out in clause [K.2.4](#)(2) of the present document for non-CRY-SOTA
937 cryptographic algorithms.

938 [\[REQ-DEFAULT-1-01\]](#) The product, in its product factory default state, shall enforce the applicable requirements of
939 the present document. The product need not enforce a requirement when (i) that requirement renders the initial product
940 setup process non-functional; and (ii) the instructions to the user document the exception.

941 [\[REQ-DEFAULT-1-02\]](#) The product, in its product factory default state, shall enable only those interfaces and services
942 that product setup requires.

943 NOTE: Some products in their product factory default state limit which network interfaces can be used for
944 product setup. Other products place no restrictions on which network interfaces can be used for product
945 setup.

946 [\[REQ-DEFAULT-1-03\]](#) The product, in its product factory default state, shall restrict access to management accounts
947 and methods, as documented in the instructions to the user.

948 [\[REQ-DEFAULT-1-04\]](#) The product, in its product operational state, shall require authenticated and authorized access
949 to management accounts.

950 [\[REQ-DEFAULT-1-05\]](#) The product, in its product factory default state, shall disable all diagnostic interfaces.

951 [\[REQ-DEFAULT-1-06\]](#) The product shall require authentication and authorization for any management action that
952 enables a diagnostic interface.

953 [\[REQ-DEFAULT-1-07\]](#) The product, in its product factory default state, shall generate audit events for (i)
954 authentication attempts; (ii) configuration changes; and (iii) product errors, if those do not affect the recording.

955 [\[REQ-DEFAULT-1-08\]](#) The product, in its product factory default state, shall require state of the art cryptography for
956 all cryptographic functions.

957 [\[REQ-DEFAULT-1-09\]](#) The product, in its product factory default state, shall (i) not enable any network-accessible
958 service that relies on a legacy protocol; and (ii) require an explicit management action to activate a legacy protocol.

959 [\[REQ-DEFAULT-1-10\]](#) Where the product has activated a legacy protocol it supports, the product shall provide a user-
960 facing indication that the legacy protocol is in use.

961 NOTE: For the present context, the mitigations recognized in publicly available specifications or in guidance
962 from a recognized body should be preferred. Recognized bodies include those listed in clause K.1.1(ii) of
963 the present document, together with IETF Best Current Practice documents and applicable ETSI
964 Technical Specifications.

965 [\[REQ-DEFAULT-1-11\]](#) Where the product supports a legacy protocol, the manufacturer shall record (i) the protocol;
966 (ii) security features no longer considered state of the art; (iii) legacy systems requiring it; and (iv) the constraint
967 preventing a state of the art alternative.

968 NOTE: For the present context, the record forms part of the technical documentation referred to in Annex VII of
969 Regulation (EU) 2024/2847.

970 [\[REQ-DEFAULT-1-12\]](#) The product shall enforce the principle of least privilege during normal operation.

971 [\[REQ-DEFAULT-1-13\]](#) The product shall store audit events in persistent memory that survives a reboot.

972 5.4.2 [RESET-1] Factory reset

973 5.4.2.1 General

974 Factory reset mechanisms remove all data and user configurations while leaving the current running software and the
975 firmware versions in place. The factory reset also deletes the user login credentials, leading to the initial setup
976 procedures.

977 NOTE: Factory reset does not include other types of reset procedures, such as what is commonly known as
978 "operational reset" or "operator reset", where user data and configuration are preserved.

979 5.4.2.2 Requirements

980 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (b).

981 [\[REQ-RESET-1-01\]](#) The product shall provide a factory reset mechanism that restores the product to its secure-by-
982 default configuration.

983 NOTE: The product can provide a physical factory reset mechanism that does not require authentication.

984 [\[REQ-RESET-1-02\]](#) The product shall provide a factory reset mechanism that maintains the currently installed
985 firmware version and all installed security updates.

986 [\[REQ-RESET-1-03\]](#) The product shall not retain (i) not-default configuration; (ii) user data; or (iii) user-instantiated or
987 modified critical security parameters after factory reset.

988 NOTE: Connection information to an ISP administrated product belongs to the default configuration information.

989 5.5 Secure updates

990 5.5.1 [UPDATE-1] Update mechanisms

991 5.5.1.1 General

992 This clause establishes requirements for delivering and installing security updates to address vulnerabilities throughout
993 the product lifetime. Products may remain deployed for extended periods and may serve as critical infrastructure.
994 Robust update mechanisms maintain security against evolving threats.

995 5.5.1.2 Requirements

996 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (c).

997 [\[REQ-UPDATE-1-01\]](#) The product shall provide a mechanism to receive security updates.

998 [\[REQ-UPDATE-1-02\]](#) The product shall prevent installation of security updates without authentication and
999 authorization.

1000 [\[REQ-UPDATE-1-03\]](#) The product shall install a received security update and report the installed version.

1001 [\[REQ-UPDATE-1-04\]](#) When the product is not designed for configuration and maintenance by professional network
1002 administrators, the product shall automatically check for security remedy updates according to the documented default
1003 schedule. Otherwise, the procedure for checking for security updates shall be included in the instructions to the user.

1004 [\[REQ-UPDATE-1-05\]](#) When the product is not designed for configuration and maintenance by professional network
1005 administrators, the security update mechanism shall be automated and enabled by default. Otherwise, the procedure for
1006 performing the security update shall be included in the instructions to the user.

1007 [\[REQ-UPDATE-1-06\]](#) The product shall verify security update integrity using state of the art cryptography before
1008 installation.

1009 [\[REQ-UPDATE-1-07\]](#) The product shall generate audit events for (i) security update availability; (ii) security update
1010 download initiation, completion, or failure; and (iii) security update installation success or failure.

1011 5.6 Authentication and access control

1012 5.6.1 [AUTH-1] Authentication

1013 5.6.1.1 General

1014 Authentication is the fundamental security barrier against product modification without authorization. These products
1015 play a critical role in network connectivity and data routing. Compromise of access controls can lead to network
1016 disruption, data interception, or malicious traffic redirection. This clause establishes requirements to ensure only
1017 authorized users can access product management functions.

1018 5.6.1.2 Requirements

1019 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (d).

1020 [\[REQ-AUTH-1-01\]](#) The product shall require user authentication on all interfaces providing management access to the
1021 product.

1022 [\[REQ-AUTH-1-02\]](#) The product shall eliminate shared default credentials by either (i) generating credentials during
1023 secure production; (ii) enforcing mandatory credential creation during initial setup; or (iii) using non-password based
1024 authentication credentials.

1025 NOTE: The generation of qualified individual user credentials can be supported by a product feature, or the
1026 product supports credential import.

1027 [\[REQ-AUTH-1-03\]](#) Where the product transmits critical security parameters, the product shall protect their
1028 transmission over a secure channel.

1029 [\[REQ-AUTH-1-04\]](#) The product shall protect critical security parameters using state of the art cryptography.

1030 [\[REQ-AUTH-1-05\]](#) When supporting password-based credentials, the product shall enforce minimum credential
1031 entropy.

1032 NOTE: Minimum credential entropy can be achieved by character complexity and minimum length requirements.

1033 [\[REQ-AUTH-1-06\]](#) The product shall enforce authentication failure protection, including (i) progressive delays
1034 between failed attempts; and (ii) temporary account lockout after a configurable number of failed attempts.

1035 [\[REQ-AUTH-1-07\]](#) When supporting password-based credentials, the product shall support maintaining the history of
1036 previously used passwords, in their processed form, to prevent reuse. The minimal number of previous passwords that
1037 shall be kept is one. The manufacturer may enable the user configuration of password history limit or increase this
1038 default based on the risk assessment. Password changes shall be validated against the configured password history limit
1039 before acceptance.

1040 5.6.2 [AUTH-2] Authorization

1041 5.6.2.1 General

1042 This clause establishes requirements for controlling what authenticated users can do on the product. While
1043 authentication verifies user identity, authorization ensures users can only perform actions permitted by their privilege
1044 level. This is critical for the product as different users require different privileges.

1045 5.6.2.2 Requirements

1046 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (d).

1047 [\[REQ-AUTH-2-01\]](#) Where the product supports more than one privilege level, the product shall enforce privilege
1048 separation.

1049 [\[REQ-AUTH-2-02\]](#) The product shall restrict each user to their authorized privilege level.

1050 [\[REQ-AUTH-2-03\]](#) The product shall enforce authorization control on all interfaces providing management access to
1051 the product.

1052 [\[REQ-AUTH-2-04\]](#) The product shall deny execution of any command that is not authorized for the privilege level of
1053 the user issuing it.

1054 5.6.3 [AUTH-3] Authenticated session lifecycle

1055 5.6.3.1 General

1056 This clause establishes requirements for managing the lifecycle of authenticated sessions, from establishment through
1057 termination. The product maintains the security context created through authentication as specified in clause [5.6.1](#) and
1058 authorization as specified in clause [5.6.2](#) throughout the interaction. Session management prevents access without
1059 authorization through session compromise.

1060 Products remain accessible continuously and may be managed from multiple locations and interfaces. Robust session
1061 controls prevent configuration changes without authorization that could compromise entire network segments.
1062 Vulnerabilities such as session hijacking, fixation, or replay attacks can lead to full product compromise, even when
1063 strong authentication is in place.

1064 5.6.3.2 Requirements

1065 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (d).

1066 Where risk factor [RF-M-02] is present, requirement [REQ-AUTH-3-01] applies.

1067 [\[REQ-AUTH-3-01\]](#) The product shall generate cryptographically secure management session identifiers using state of
1068 the art cryptography. Session identifiers shall be unique, non-predictable, and resistant to brute force attacks.

1069 Where any of risk factors [RF-M-02], [RF-M-03], [RF-M-04] is present, requirement [REQ-AUTH-3-02] applies.

1070 [\[REQ-AUTH-3-02\]](#) The product shall enforce session timeout with configurable idle timeout periods and default
1071 values.

1072 Where any of risk factors [RF-M-02], [RF-M-03], [RF-M-04] is present, requirement [REQ-AUTH-3-03] applies.

1073 [\[REQ-AUTH-3-03\]](#) The product shall invalidate sessions immediately upon (i) user-initiated logout; (ii) timeout
1074 expiration; (iii) authentication credential change; (iv) expiry of a credential's validity; or (v) management termination.
1075 Session invalidation shall securely remove all session data.

1076 Where any of risk factors [RF-M-02], [RF-M-03], [RF-M-04] is present, requirement [REQ-AUTH-3-04] applies.

1077 [\[REQ-AUTH-3-04\]](#) The product shall protect session identifiers by (i) transmitting them only over secure channels
1078 using state of the art cryptography; (ii) implementing session token protection mechanisms; and (iii) preventing
1079 disclosure of session identifiers in any product output.

1080 Where any of risk factors [RF-M-02], [RF-M-03], [RF-M-04] is present, requirement [REQ-AUTH-3-05] applies.

1081 [\[REQ-AUTH-3-05\]](#) The product shall limit concurrent sessions to a configurable maximum per user account.

1082 Where any of risk factors [RF-M-02], [RF-M-03], [RF-M-04] is present, requirement [REQ-AUTH-3-06] applies.

1083 [\[REQ-AUTH-3-06\]](#) The product shall deny privilege escalation attempts without authorization within active sessions.

1084 5.6.4 [AUTH-4] Protocol access control

1085 5.6.4.1 General

1086 This clause establishes requirements for management control over network protocols available on the product. Only
1087 authenticated and authorized users can enable, disable, or configure network protocols. Once enabled by an authorized
1088 user, protocols may operate according to their specifications. This applies to protocols that inherently lack
1089 authentication mechanisms for protocol-level interactions.

1090 5.6.4.2 Requirements

1091 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (d).

1092 Where risk factor [RF-P-01] is present, requirement [REQ-AUTH-4-01] applies.

1093 [\[REQ-AUTH-4-01\]](#) The product shall enable only management protocols using state of the art cryptography in product
1094 factory default state and in product operational state.

1095 Where risk factor [RF-P-02] is present, requirement [REQ-AUTH-4-02] applies.

1096 [\[REQ-AUTH-4-02\]](#) The product shall implement rate limiting and source validation for unauthenticated protocol
1097 requests to mitigate DoS attacks against management plane and control plane interfaces.

1098 NOTE: The specific operational state for this assessment includes but is not limited to operational state prior to
1099 DoS conditions.

1100 Where risk factor [RF-P-03] is present, requirement [REQ-AUTH-4-03] applies.

1101 [\[REQ-AUTH-4-03\]](#) The product shall provide capability to configure state of the art cryptography and to disable
1102 protocols that do not use state of the art cryptography.

1103 Where risk factor [RF-P-04] is present, requirement [REQ-AUTH-4-04] applies.

1104 [\[REQ-AUTH-4-04\]](#) The product shall (i) validate trust establishment using additional mechanisms; and (ii) generate
1105 audit events for all trust relationship changes.

1106 5.7 Data protection

1107 5.7.1 General

1108 This clause establishes requirements for data confidentiality, integrity, and minimization throughout the product
1109 lifecycle. Data protection rests on three principles. Confidentiality ensures data is accessible only to authorized entities.
1110 Integrity ensures data cannot be modified without authorization. Data minimization limits collection and retention to
1111 what the intended functions require. These principles apply to all data types processed by the product. Security controls
1112 prevent passive interception and active manipulation of data.

1113 NOTE 1: Data necessary for intended routing, switching, or modem functions, or for any additional product
1114 capabilities described in clause [4.2.6](#), includes IP routing tables, ARP/MAC address tables, DHCP lease
1115 records, NAT state, firewall session state, and DNS forwarding data. It also includes WAN session
1116 parameters, spanning tree and discovery protocol data, QoS metadata, and network configuration
1117 parameters such as SSIDs, VLAN assignments, and access control lists.

1118 NOTE 2: Data considered beyond the intended purpose includes long-term retention of DNS queries or visited
1119 URLs, and deep packet inspection payloads kept beyond real-time traffic management. Further examples
1120 are per-device behavioural analytics such as usage patterns or browsing habits, device fingerprinting
1121 beyond what DHCP and access control require, and diagnostic or telemetry data sent to the manufacturer
1122 or third parties.

1123 5.7.2 Requirements

1124 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (e), (2) (f) and (2) (g).

1125 [\[REQ-DATA-1-01\]](#) The product shall protect the confidentiality of data at rest by one or more of the following: (i)
1126 encryption of the data using CRY-SOTA cryptography (see Annex K); (ii) access controls that prevent read access to
1127 the stored data by unauthorized entities; or (iii) another technical means that provides protection of data-at-rest
1128 confidentiality against unauthorized disclosure equivalent to (i) or (ii), where the product's technical documentation
1129 identifies the means and demonstrates how that protection is achieved.

1130 NOTE 1: Point (iii) reflects the CRA [\[i.1\]](#), Annex I, Part I, point (2)(e), under which confidentiality may be
1131 protected by encryption or by other technical means. Point (iii) is technology-neutral and presupposes no
1132 specific implementation; examples include constructions in which the data is present in readable form
1133 only transiently during operation, or in which no interface exposes a command to read out the stored data.

1134 NOTE 2: Where the demonstration under point (iii) is not provided, or is not sufficient to establish protection
1135 equivalent to point (i) or point (ii), the data at rest cannot be considered protected and is assessed under
1136 [\[AC-DATA-1-01\]](#) as if stored in plaintext.

1137 [\[REQ-DATA-1-02\]](#) The product shall protect management communications and control plane traffic using state of the
1138 art cryptography.

1139 [\[REQ-DATA-1-03\]](#) The product shall prevent modification of configuration and firmware without authorization.

1140 [\[REQ-DATA-1-04\]](#) The product shall implement data protection measures ensuring the product processes and retains
1141 only the minimum data necessary for its intended (i) routing; (ii) switching; (iii) modem functions; or (iv) any
1142 additional product capabilities, including those described in clause [4.2.6](#).

1143 [\[REQ-DATA-1-05\]](#) The product shall require explicit opt-in configuration of any diagnostic or telemetry data collection
1144 beyond the product's intended purpose, with such collection disabled by default.

1145 5.8 Availability and resilience

1146 5.8.1 General

1147 This clause establishes requirements for maintaining product functions and protecting against service disruptions and
1148 DoS attacks. Availability and resilience address two core objectives. The first is operational continuity during and after
1149 security incidents. The second is preventing the product from being used to disrupt other networks or services. Products
1150 detect, withstand, and recover from attacks while preserving core network operations.

1151 5.8.2 Requirements

1152 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (h) and (2) (i).

1153 [\[REQ-AVAIL-1-01\]](#) The product shall enforce rate limiting for each network protocol terminated by the product.

1154 NOTE: The specific operational state for this assessment includes but is not limited to operational state prior to
1155 DoS conditions.

1156 [\[REQ-AVAIL-1-02\]](#) The product shall enforce connection throttling for each connection-oriented network protocol
1157 terminated by the product.

1158 NOTE: The specific operational state for this assessment includes but is not limited to operational state prior to
1159 DoS conditions.

1160 [\[REQ-AVAIL-1-03\]](#) The product shall automatically recover to specific operational state when DoS conditions cease,
1161 without requiring manual intervention.

1162 [\[REQ-AVAIL-1-04\]](#) The product shall generate audit events when (i) resource utilization exceeds the documented high
1163 utilization threshold and (ii) resource utilization returns below the documented high utilization threshold.

1164 NOTE: The high utilization threshold levels are an implementation option and can be set by the manufacturer or
1165 be available as a user-configurable setting.

1166 5.9 Attack surface and mitigation

1167 5.9.1 [INTEGRITY-1] System integrity and boot process

1168 5.9.1.1 General

1169 This clause establishes requirements for product integrity throughout the operational lifecycle, from initial power-on
1170 through runtime operation. System integrity is the foundational trust anchor on which all other security controls depend.
1171 A compromised boot process or runtime environment can subvert authentication, bypass access controls, and grant
1172 persistent access without authorization that survives reboots and firmware updates.

1173 The boot process is a critical attack surface for persistent implants, security control bypass, and extraction of
1174 cryptographic material. Products operate autonomously for extended periods and control critical network functions.
1175 Boot integrity and runtime security prevent attacks during these periods and thus can prevent the compromise of entire
1176 network segments.

1177 5.9.1.2 Requirements

1178 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (k).

1179 [\[REQ-INTEGRITY-1-01\]](#) The product shall verify boot component integrity using state of the art cryptography.

1180 [\[REQ-INTEGRITY-1-02\]](#) The product shall in the factory default state enforce a secure boot chain where (i) each stage
1181 of the boot chain verifies the next stage before transferring execution control; (ii) the trusted code which is the first

1182 stage of the secure boot chain is protected against unauthorized modification; (iii) the product enters a predefined failure
1183 state on verification failure; and (iv) only verified code executes during boot.

1184 NOTE 1: The product can provide a management mechanism by which the initial or subsequent trust materials used
1185 for enforcing the trust chain can be changed by at least, but not limited to, the authorized user.

1186 NOTE 2: The verification can be based on cryptographic signatures, hashes or measured boot.

1187 [\[REQ-INTEGRITY-1-03\]](#) The product shall generate audit events for all boot events including (i) boot stage
1188 progression; (ii) verification, either success or failure, for each component; (iii) recovery mode activation; and (iv)
1189 detected bypass attempts.

1190 NOTE: The generation of audit events at booting phases has constraints as the corresponding functionalities are
1191 not operational at this stage. An integrity error through these early phases is constrained by the absence of
1192 essential components and causes execution to halt or triggers a hard reset. As a consequence, audit events
1193 for such early errors cannot be generated as no memory is yet available for writing.

1194 [\[REQ-INTEGRITY-1-04\]](#) The product shall protect recovery and maintenance modes by using methods documented in
1195 the instructions to the user.

1196 5.9.2 [PACKET-1] Default packet disposition

1197 5.9.2.1 General

1198 Products implement packet processing through various approaches for their intended deployments. Validation covers
1199 standardized protocols and expected traffic, but all conceivable packet constructions cannot be validated in advance.
1200 Packets with unexpected protocol combinations, unusual encapsulations, or deeply nested tunnelling may fall outside
1201 validated processing paths. When packet processing encounters formats with no validated path, deterministic behaviour
1202 is required to maintain security and availability. Without explicit handling, such packets can cause undefined states,
1203 memory corruption, or unpredictable behaviour.

1204 Products respond deterministically to packets outside their processing domain. Best-effort processing risks undefined
1205 behaviour in hardware acceleration engines or software stacks.

1206 This requirement applies to all products regardless of deployment. The inability to handle unexpected packets safely is a
1207 fundamental vulnerability exploitable from any network position. Products drop packets rather than forward or process
1208 them when the correct action cannot be determined.

1209 5.9.2.2 Requirements

1210 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (j).

1211 [\[REQ-PACKET-1-01\]](#) The product shall drop any packet for which it cannot determine any processing action that is
1212 based on implemented protocol handlers, forwarding rules, or state machines. This includes (i) packets with
1213 unrecognized protocol identifiers or type fields; (ii) packets with invalid or unexpected encapsulation combinations; (iii)
1214 packets that require processing beyond the implemented protocol stack depth of the product; (iv) packets whose header
1215 field values fall outside the ranges specified by applicable protocol standards; (v) packets that do not match existing
1216 connection state for stateful protocols; and (vi) any packet that triggers undefined behaviour in the product.

1217 5.9.3 [EXPOSURE-1] Interface and service exposure minimization

1218 5.9.3.1 General

1219 This clause establishes requirements to limit exposed interfaces and services. Products expose only what their intended
1220 operation requires. Each exposed interface is an attack vector; reducing unnecessary exposure reduces risk.

1221 5.9.3.2 Requirements

1222 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (j).

1223 [\[REQ-EXPOSURE-1-01\]](#) The product shall enable only those interfaces and services that have been configured,
1224 regardless of the product state.

1225 [\[REQ-EXPOSURE-1-02\]](#) The product shall provide capability to selectively enable or disable individual services and
1226 interfaces through configuration.

1227 5.10 Monitoring and logging

1228 5.10.1 General

1229 This clause covers requirements for recording and monitoring. Records support incident detection, forensic analysis,
1230 and compliance checks. The following activities are logged: authentication attempts, configuration changes, system
1231 events, and management actions. Event data is protected against modification or deletion without authorization.
1232 Retention periods and logging scope are set based on operational needs and resource constraints.

1233 5.10.2 Requirements

1234 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (l).

1235 [\[REQ-LOG-1-01\]](#) The product shall generate audit events for authentication activities including but not limited to (i)
1236 successful or failed authentication; (ii) account lockout triggers and releases; and (iii) authentication credential change
1237 attempts.

1238 [\[REQ-LOG-1-02\]](#) The product shall generate audit events for all session lifecycle activities including (i) session
1239 establishment with source details; (ii) session termination with reason; (iii) failed session validation attempts; and (iv)
1240 concurrent session limit violations.

1241 [\[REQ-LOG-1-03\]](#) The product shall implement command authorization that generates audit events whenever execution
1242 of unauthorized command is requested.

1243 5.11 Data management

1244 5.11.1 [TRANSFER-1] Secure data export and transfer

1245 5.11.1.1 General

1246 This clause addresses secure data transfer between products. Users require the ability to migrate configurations,
1247 operational data, and system state without loss of security. Configuration files contain critical security parameters and
1248 need protection during export and transfer.

1249 NOTE: This does not limit the choice of users to import or export data using legacy protocols maintained for
1250 backward compatibility.

1251 5.11.1.2 Requirements

1252 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (m).

1253 [\[REQ-TRANSFER-1-01\]](#) The product shall provide capability to transfer exported data over a channel protected by
1254 state of the art cryptography.

1255 [\[REQ-TRANSFER-1-02\]](#) The product shall provide capability to transfer imported data over a channel protected by
1256 state of the art cryptography.

1257 [\[REQ-TRANSFER-1-03\]](#) The product shall require management access for data export and data import operations.

1258 [\[REQ-TRANSFER-1-04\]](#) The product shall generate audit events for all data export and data import operations.

1259

1260 6 Assessment criteria for compliance with technical 1261 requirements

1262 6.1 Introduction to the assessment and compliance criteria

1263 This clause details the assessment process for compliance with the requirements in clause 5 of the present document.

1264 NOTE: In the following clauses, *documentation* means any documentation provided to the assessor. This
1265 includes, but is not limited to, the technical specification, test results, and instructions to the user.

1266 6.2 No known exploitable vulnerabilities

1267 6.2.1 [KEV-1] No known exploitable vulnerabilities

1268 6.2.1.1 Requirement assessments

1269 [\[AC-KEV-1-01\]](#) Verify that the manufacturer maintains a software bill of materials for each product version in a
1270 machine-readable format.

1271 **Assessment reference**

1272 Requirement [\[REQ-KEV-1-01\]](#).

1273 **Assessment objective**

1274 Confirm that the manufacturer maintains a software bill of materials whose declared version matches the installed
1275 version reported by the product.

1276 **Assessment preparation**

- 1277 1. The product is in specific operational state.
- 1278 2. The software bill of materials for the product is available.
- 1279 3. Documentation describing the software bill of materials maintenance process is available.

1280 **Assessment activities**

- 1281 1. Review documentation to identify the software bill of materials maintenance process.
- 1282 2. Inspect the software bill of materials and the installed version reported by the product. Verify that the version
1283 declared in the software bill of materials matches the installed version reported by the product.

1284 **Assessment verdict**

1285 The verdict fail is assigned if any of the following conditions apply:

- 1286 1. Documentation does not describe the software bill of materials maintenance process.
- 1287 2. The manufacturer does not maintain a software bill of materials whose declared version matches the installed
1288 version reported by the product.

1289 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1290 1. Documentation describes the software bill of materials maintenance process.
- 1291 2. The manufacturer maintains a software bill of materials whose declared version matches the installed version
1292 reported by the product.

1293 **Assessment evidence**

- 1294 1. Documentation describing the software bill of materials maintenance process.
- 1295 2. The software bill of materials and the installed version reported by the product.

1296

1297 [\[AC-KEV-1-02\]](#) Verify that the product contains no known exploitable vulnerabilities in each product version when
1298 made available on the market.

1299 **Assessment reference**

1300 Requirement [\[REQ-KEV-1-02\]](#).

1301 **Assessment objective**

1302 Confirm that no component of the product contains a known exploitable vulnerability in each product version when
1303 made available on the market.

1304 **Assessment preparation**

- 1305 1. The product is in product factory default state.
1306 2. Documentation describing the vulnerability assessment process is available.
1307 3. The software bill of materials is available.

1308 **Assessment activities**

- 1309 1. Review the software bill of materials. Verify that all product components and third-party dependencies are
1310 listed with version identifiers.
1311 2. Cross-reference each component in the software bill of materials against known vulnerability databases. Verify
1312 that no listed component has a known exploitable vulnerability at the time of assessment.
1313 3. Verify that the software bill of materials is maintained in a machine-readable format.

1314 **Assessment verdict**

1315 The verdict fail is assigned if any of the following conditions apply:

- 1316 1. The product does not provide a software bill of materials that lists all product components and third-party
1317 dependencies with version identifiers.
1318 2. The product contains a known exploitable vulnerability in one or more components listed in the software bill
1319 of materials.
1320 3. The product does not provide a software bill of materials in a machine-readable format.

1321 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1322 1. The product provides a software bill of materials that lists all product components and third-party
1323 dependencies with version identifiers.
1324 2. The product does not contain a known exploitable vulnerability in any component listed in the software bill of
1325 materials.
1326 3. The product provides a software bill of materials in a machine-readable format.

1327 **Assessment evidence**

- 1328 1. Documentation showing the software bill of materials lists all product components and third-party
1329 dependencies with version identifiers.
1330 2. Test results showing no component listed in the software bill of materials contains a known exploitable
1331 vulnerability.
1332 3. Documentation showing the format of the software bill of materials.
1333

1334 [\[AC-KEV-1-03\]](#) Verify that the manufacturer verifies third-party components against known vulnerability databases
1335 before making each product version available on the market.

1336 **Assessment reference**

1337 Requirement [\[REQ-KEV-1-03\]](#).

1338 **Assessment objective**

1339 Confirm that the manufacturer verifies third-party components against known vulnerability databases before each
1340 release.

1341 **Assessment preparation**

- 1342 1. Documentation describing the third-party component verification process is available.
1343 2. The software bill of materials is available.

1344 **Assessment activities**

- 1345 1. Review documentation to identify the process for verifying third-party components against vulnerability
 1346 databases before making each product version available on the market.
 1347 2. Inspect the software bill of materials and verify that each third-party component is listed with a version
 1348 identifier and has been checked against vulnerability databases.

1349 **Assessment verdict**

1350 The verdict fail is assigned if any of the following conditions apply:

- 1351 1. Documentation does not describe the third-party component verification process.
 1352 2. Any third-party component lacks a version identifier or has not been verified against vulnerability databases.

1353 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1354 1. Documentation describes the third-party component verification process.
 1355 2. All third-party components are listed with version identifiers and verified against vulnerability databases.

1356 **Assessment evidence**

- 1357 1. Documentation describing the third-party component verification process.
 1358 2. Test results showing all third-party components are listed with version identifiers and verified against
 1359 vulnerability databases.
 1360

1361 **6.3 Secure by default configuration**

1362 **6.3.1 [DEFAULT-1] Secure by default configuration**

1363 **6.3.1.1 Requirement assessments**

1364 [\[AC-DEFAULT-1-01\]](#) Verify that the product enforces the applicable requirements of the present document in product
 1365 factory default state, and that each excepted requirement (i) renders the initial product setup process non-functional; and
 1366 (ii) the instructions to the user document the exception.

1367 **Assessment reference**

1368 Requirement [\[REQ-DEFAULT-1-01\]](#).

1369 **Assessment objective**

1370 Confirm that the product enforces the applicable requirements of the present document in product factory default state,
 1371 and that each excepted requirement (i) renders the initial product setup process non-functional; and (ii) the instructions
 1372 to the user document the exception.

1373 **Assessment preparation**

- 1374 1. The product is in product factory default state.
 1375 2. Documentation listing applicable requirements and their conformance status in product factory default state is
 1376 available.
 1377 3. Instructions to the user are available.

1378 **Assessment activities**

- 1379 1. Review documentation to identify the applicable requirements that are excepted from product factory default
 1380 state.
 1381 2. Review documentation for each excepted requirement to confirm the stated justification that conforming to it
 1382 renders the initial product setup process non-functional.
 1383 3. Inspect the product in product factory default state to identify all requirements that are not conformed to.
 1384 Verify that each non-conformed requirement is listed in documentation as excepted.
 1385 4. Inspect the product in product factory default state to verify that all non-excepted requirements are conformed
 1386 to.
 1387 5. Enforce conformance to each excepted requirement individually and attempt setup. Verify that setup fails.
 1388 6. Review instructions to the user to verify that each excepted requirement is listed.

1389 **Assessment verdict**

1390 The verdict fail is assigned if any of the following conditions apply:

- 1391 1. Documentation does not list all applicable requirements excepted from product factory default state.
- 1392 2. Documentation does not describe the justification that conforming to each excepted requirement renders the
- 1393 initial product setup process non-functional.
- 1394 3. The product does not document any non-conformed requirement in product factory default state as excepted.
- 1395 4. Any non-excepted requirement is not conformed to in product factory default state.
- 1396 5. The product does not fail setup when any excepted requirement is individually enforced.
- 1397 6. Instructions to the user do not document every excepted requirement.

1398 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1399 1. Documentation lists all applicable requirements excepted from product factory default state.
- 1400 2. Documentation describes the justification that conforming to each excepted requirement renders the initial
- 1401 product setup process non-functional.
- 1402 3. The product documents every non-conformed requirement in product factory default state as excepted.
- 1403 4. All non-excepted requirements are conformed to in product factory default state.
- 1404 5. The product fails setup when each excepted requirement is individually enforced.
- 1405 6. Instructions to the user document every excepted requirement.

1406 **Assessment evidence**

- 1407 1. Documentation listing all applicable requirements excepted from product factory default state.
- 1408 2. Documentation describing the justification that conforming to each excepted requirement renders the initial
- 1409 product setup process non-functional.
- 1410 3. Test results showing the product documents every non-conformed requirement in product factory default state
- 1411 as excepted.
- 1412 4. Test results showing all non-excepted requirements are conformed to in product factory default state.
- 1413 5. Test results showing setup failure when each excepted requirement is individually enforced.
- 1414 6. Instructions to the user listing all excepted requirements.
- 1415

1416 [\[AC-DEFAULT-1-02\]](#) Verify that the product, in its product factory default state, enables only those interfaces and
1417 services that product setup requires.

1418 **Assessment reference**

1419 Requirement [\[REQ-DEFAULT-1-02\]](#).

1420 **Assessment objective**

1421 Confirm that the product enables only the interfaces and services that product setup requires in product factory default
1422 state, and that no additional interfaces or services are active.

1423 **Assessment preparation**

- 1424 1. The product is in product factory default state.
- 1425 2. Documentation describing the network interfaces and services required for product setup is available.

1426 **Assessment activities**

- 1427 1. Review documentation to identify all network interfaces and services required for product setup.
- 1428 2. Inspect the product in product factory default state. Verify the product enables only network interfaces and
- 1429 services documented as required for setup and does not initiate undocumented outbound connections.
- 1430 3. Complete the product setup process using only the documented interfaces and services. Verify that setup
- 1431 succeeds.
- 1432 4. Attempt to access a network interface or service not documented as required for setup in product factory
- 1433 default state. Verify that access is denied or the interface is inactive.

1434 **Assessment verdict**

1435 The verdict fail is assigned if any of the following conditions apply:

- 1436 1. Documentation does not list all interfaces and services required for product setup.
- 1437 2. Any active network interface in product factory default state is not documented as required for setup.

- 1438 3. Any listening network service in product factory default state is not documented as required for setup.
 1439 4. The product initiates an undocumented outbound connection in product factory default state.
 1440 5. The product does not complete setup successfully using only documented interfaces and services.
 1441 6. The product does not deny access to network interfaces and services not required for setup in product factory
 1442 default state.

1443 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1444 1. Documentation lists all interfaces and services required for product setup.
 1445 2. All active network interfaces in product factory default state are documented as required for setup.
 1446 3. All listening network services in product factory default state are documented as required for setup.
 1447 4. The product does not initiate any undocumented outbound connection in product factory default state.
 1448 5. The product completes setup successfully using only documented interfaces and services.
 1449 6. The product denies access to network interfaces and services not required for setup in product factory default
 1450 state.

1451 **Assessment evidence**

- 1452 1. Documentation listing all interfaces and services required for product setup.
 1453 2. Test results showing all active network interfaces in product factory default state are documented as required
 1454 for setup.
 1455 3. Test results showing all listening network services in product factory default state are documented as required
 1456 for setup.
 1457 4. Test results showing the product does not initiate any undocumented outbound connection in product factory
 1458 default state.
 1459 5. Test results showing setup completes successfully using only documented interfaces and services.
 1460 6. Test results showing non-setup network interfaces and services are inaccessible in product factory default state.
 1461

1462 [\[AC-DEFAULT-1-03\]](#) Verify that the product, in its product factory default state, restricts access to management
 1463 accounts and methods, as documented in the instructions to the user.

1464 **Assessment reference**

1465 Requirement [\[REQ-DEFAULT-1-03\]](#).

1466 **Assessment objective**

1467 Confirm that the product restricts access to management accounts and methods as documented in the instructions to the
 1468 user, and that no undocumented management accounts or access methods exist.

1469 **Assessment preparation**

- 1470 1. The product is in product factory default state.
 1471 2. Instructions to the user describing factory default management accounts and methods are available.

1472 **Assessment activities**

- 1473 1. Review instructions to the user to identify all factory default management accounts and methods.
 1474 2. Attempt access using each management account and method documented in the instructions to the user. Verify
 1475 that access is granted.
 1476 3. Attempt access using management accounts and methods not documented in the instructions to the user. Verify
 1477 that the product restricts access by denying undocumented management accounts and methods.

1478 **Assessment verdict**

1479 The verdict fail is assigned if any of the following conditions apply:

- 1480 1. Instructions to the user do not identify all factory default management accounts and methods.
 1481 2. Any management account or method documented in the instructions to the user is not functional in product
 1482 factory default state.
 1483 3. The product does not deny access using undocumented management accounts and methods.

1484 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1485 1. Instructions to the user identify all factory default management accounts and methods.

- 1486 2. All management accounts and methods documented in the instructions to the user are functional in product
 1487 factory default state.
 1488 3. The product denies access using undocumented management accounts and methods.

1489 **Assessment evidence**

- 1490 1. Instructions to the user listing all factory default management accounts and methods.
 1491 2. Test results showing all management accounts and methods documented in the instructions to the user are
 1492 functional in product factory default state.
 1493 3. Test results showing undocumented management accounts and methods are denied.
 1494

1495 [\[AC-DEFAULT-1-04\]](#) Verify that the product, in its product operational state, requires authenticated and authorized
 1496 access to management accounts.

1497 **Assessment reference**

1498 Requirement [\[REQ-DEFAULT-1-04\]](#).

1499 **Assessment objective**

1500 Confirm that access to management accounts in product operational state is granted only after successful authentication
 1501 and that the authenticated identity is authorized for the requested management account.

1502 **Assessment preparation**

- 1503 1. The product is in product operational state with at least one management account configured by the user.
 1504 2. Documentation describing authentication and authorization mechanisms for management accounts is available.

1505 **Assessment activities**

- 1506 1. Review documentation to identify authentication and authorization mechanisms applied to management
 1507 accounts.
 1508 2. Attempt access to a management account using valid authentication credentials of an identity authorized for
 1509 that account. Verify that access is granted.
 1510 3. Attempt access to a management account without providing authentication credentials or with invalid
 1511 credentials. Verify that the product denies access.
 1512 4. Attempt access to a management account using valid authentication credentials of an identity that is not
 1513 authorized for that account. Verify that the product denies access.

1514 **Assessment verdict**

1515 The verdict fail is assigned if any of the following conditions apply:

- 1516 1. Documentation does not describe authentication and authorization mechanisms applied to management
 1517 accounts.
 1518 2. The product does not grant access to the management account when authentication succeeds and the
 1519 authenticated identity is authorized.
 1520 3. The product does not deny access to the management account when authentication is absent or fails.
 1521 4. The product does not deny access to the management account when the authenticated identity is not
 1522 authorized.

1523 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1524 1. Documentation describes authentication and authorization mechanisms applied to management accounts.
 1525 2. The product grants access to the management account when authentication succeeds and the authenticated
 1526 identity is authorized.
 1527 3. The product denies access to the management account when authentication is absent or fails.
 1528 4. The product denies access to the management account when the authenticated identity is not authorized.

1529 **Assessment evidence**

- 1530 1. Documentation describing authentication and authorization mechanisms for management accounts.
 1531 2. Test results showing access is granted to a management account on successful authentication and
 1532 authorization.
 1533 3. Test results showing access to a management account is denied when authentication is absent or fails.

1534 4. Test results showing access to a management account is denied when the authenticated identity is not
1535 authorized.
1536

1537 [\[AC-DEFAULT-1-05\]](#) Verify that the product disables all diagnostic interfaces in product factory default state.

1538 **Assessment reference**

1539 Requirement [\[REQ-DEFAULT-1-05\]](#).

1540 **Assessment objective**

1541 Confirm that all diagnostic interfaces are disabled in product factory default state.

1542 **Assessment preparation**

- 1543 1. The product is in product factory default state.
- 1544 2. Documentation listing all diagnostic interfaces is available.

1545 **Assessment activities**

- 1546 1. Review documentation to identify all diagnostic interfaces.
- 1547 2. Inspect the product in product factory default state to verify that each documented diagnostic interface is
1548 disabled.
- 1549 3. Attempt to access each documented diagnostic interface in product factory default state. Verify that access is
1550 denied or the interface is inactive.

1551 **Assessment verdict**

1552 The verdict fail is assigned if any of the following conditions apply:

- 1553 1. Documentation does not list all diagnostic interfaces.
- 1554 2. Any documented diagnostic interface is enabled in product factory default state.
- 1555 3. Any documented diagnostic interface does not deny access in product factory default state.

1556 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1557 1. Documentation lists all diagnostic interfaces.
- 1558 2. All documented diagnostic interfaces are disabled in product factory default state.
- 1559 3. All documented diagnostic interfaces deny access in product factory default state.

1560 **Assessment evidence**

- 1561 1. Documentation listing all diagnostic interfaces.
 - 1562 2. Test results showing all documented diagnostic interfaces are disabled in product factory default state.
 - 1563 3. Test results showing all documented diagnostic interfaces deny access in product factory default state.
- 1564

1565 [\[AC-DEFAULT-1-06\]](#) Verify that the product requires authentication and authorization for any management action that
1566 enables a diagnostic interface.

1567 **Assessment reference**

1568 Requirement [\[REQ-DEFAULT-1-06\]](#).

1569 **Assessment objective**

1570 Confirm that the product requires authentication and authorization for any management action that enables a diagnostic
1571 interface.

1572 **Assessment preparation**

- 1573 1. The product is in specific operational state.
- 1574 2. Documentation describing the management actions used to enable diagnostic interfaces is available.

1575 **Assessment activities**

- 1576 1. Review documentation to identify all management actions used to enable diagnostic interfaces.

- 1577 2. Attempt to perform each management action to enable a diagnostic interface without authentication. Verify
1578 that the product denies the action.
- 1579 3. Attempt to perform each management action to enable a diagnostic interface with credentials below the
1580 required authorization level. Verify that the product denies the action.
- 1581 4. Perform each management action to enable a diagnostic interface with credentials at the required authorization
1582 level. Verify that the action succeeds.

1583 **Assessment verdict**

1584 The verdict fail is assigned if any of the following conditions apply:

- 1585 1. Documentation does not describe all management actions used to enable diagnostic interfaces.
- 1586 2. The product does not deny access without authentication to any diagnostic interface.
- 1587 3. The product does not deny access with insufficient authorization to any diagnostic interface.
- 1588 4. The product does not grant access with authentication and authorization to any diagnostic interface.

1589 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1590 1. Documentation describes all management actions used to enable diagnostic interfaces.
- 1591 2. The product denies access without authentication to each diagnostic interface.
- 1592 3. The product denies access with insufficient authorization to each diagnostic interface.
- 1593 4. The product grants access with authentication and authorization to each diagnostic interface.

1594 **Assessment evidence**

- 1595 1. Documentation describing all management actions used to enable diagnostic interfaces.
- 1596 2. Test results showing the product denies access without authentication to each diagnostic interface.
- 1597 3. Test results showing the product denies access with insufficient authorization to each diagnostic interface.
- 1598 4. Test results showing the product grants access with authentication and authorization to each diagnostic
1599 interface.

1600

1601 [\[AC-DEFAULT-1-07\]](#) Verify that the product, in its product factory default state, generates audit events for (i)
1602 authentication attempts; (ii) configuration changes; and (iii) product errors, if those do not affect the recording.

1603 **Assessment reference**

1604 Requirement [\[REQ-DEFAULT-1-07\]](#).

1605 **Assessment objective**

1606 Confirm that the product, in its product factory default state, generates audit events for authentication attempts,
1607 configuration changes, and product errors that do not affect the recording.

1608 **Assessment preparation**

- 1609 1. The product is in product factory default state.
- 1610 2. Documentation describing audit events generated for authentication attempts, configuration changes, and
1611 product errors is available.

1612 **Assessment activities**

- 1613 1. Review documentation to identify the audit events generated for authentication attempts, configuration
1614 changes, and product errors.
- 1615 2. Trigger each authentication attempt scenario described in the documentation. Verify that the product generates
1616 an audit event for each attempt.
- 1617 3. Perform each configuration change scenario described in the documentation. Verify that the product generates
1618 an audit event for each change.
- 1619 4. Trigger each product error condition described in the documentation that does not affect audit recording.
1620 Verify that the product generates an audit event for the error.

1621 **Assessment verdict**

1622 The verdict fail is assigned if any of the following conditions apply:

- 1623 1. Documentation does not describe the audit events generated for authentication attempts, configuration
1624 changes, or product errors.

- 1625 2. The product does not generate an audit event for any authentication attempt.
 1626 3. The product does not generate an audit event for any configuration change.
 1627 4. The product does not generate an audit event for any product error that does not affect audit recording.

1628 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1629 1. Documentation describes the audit events generated for authentication attempts, configuration changes, and
 1630 product errors.
 1631 2. The product generates an audit event for each authentication attempt.
 1632 3. The product generates an audit event for each configuration change.
 1633 4. The product generates an audit event for each product error that does not affect audit recording.

1634 **Assessment evidence**

- 1635 1. Documentation describing the audit events generated for authentication attempts, configuration changes, and
 1636 product errors.
 1637 2. Test results showing the product generates audit events for each authentication attempt.
 1638 3. Test results showing the product generates audit events for each configuration change.
 1639 4. Test results showing the product generates audit events for product errors that do not affect audit recording.

1640

1641 [\[AC-DEFAULT-1-08\]](#) Verify that the product, in its product factory default state, requires state of the art cryptography
 1642 for all cryptographic functions.

1643 **Assessment reference**

1644 Requirement [\[REQ-DEFAULT-1-08\]](#).

1645 **Assessment objective**

1646 Confirm that the product, in its product factory default state, requires state of the art cryptography for all cryptographic
 1647 functions, and that no deprecated or weak cryptography is enabled.

1648 **Assessment preparation**

- 1649 1. Documentation describing the cryptographic configuration is available.

1650 **Assessment activities**

- 1651 1. Review documentation to identify the cryptographic configuration.
 1652 2. Inspect the product in product factory default state to verify the active cryptographic configuration matches the
 1653 documented cryptographic configuration and is state of the art.
 1654 3. Inspect the product in product operational state to verify the active cryptographic configuration matches the
 1655 documented cryptographic configuration and is state of the art.
 1656 4. Verify that where cryptographic negotiation is supported, the default order does not prefer deprecated
 1657 cryptography over recognized cryptography, and that where only fixed configuration is used, no negotiation
 1658 occurs.

1659 **Assessment verdict**

1660 The verdict fail is assigned if any of the following conditions apply:

- 1661 1. Documentation does not describe the cryptographic configuration.
 1662 2. The product does not use state of the art cryptography in product factory default state.
 1663 3. The product does not use state of the art cryptography in product operational state.
 1664 4. The product does not prioritize recognized cryptography over deprecated cryptography in the default
 1665 negotiation order where negotiation is supported.
 1666 5. The product performs cryptographic negotiation where only fixed configuration is used.

1667 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1668 1. Documentation describes the cryptographic configuration.
 1669 2. The product uses state of the art cryptography in product factory default state.
 1670 3. The product uses state of the art cryptography in product operational state.
 1671 4. The product prioritizes recognized cryptography over deprecated cryptography in the default negotiation order
 1672 where negotiation is supported.

1673 5. The product does not perform cryptographic negotiation where only fixed configuration is used.

1674 **Assessment evidence**

- 1675 1. Documentation describing the cryptographic configuration.
- 1676 2. Test results showing the cryptographic configuration is state of the art in product factory default state.
- 1677 3. Test results showing the cryptographic configuration is state of the art in product operational state.
- 1678 4. Test results showing the default negotiation order does not prefer deprecated cryptography over recognized cryptography where negotiation is supported.
- 1679 5. Test results showing no cryptographic negotiation occurs where only fixed configuration is used.

1681

1682 [\[AC-DEFAULT-1-09\]](#) Verify that the product, in its product factory default state, does not enable any network-
 1683 accessible service that relies on a legacy protocol, and that activation of a legacy protocol requires an explicit
 1684 management action.

1685 **Assessment reference**

1686 Requirement [\[REQ-DEFAULT-1-09\]](#).

1687 **Assessment objective**

1688 Confirm that the product enables no network-accessible service that relies on a legacy protocol in product factory
 1689 default state, and that the product requires an explicit management action to activate a legacy protocol.

1690 **Assessment preparation**

- 1691 1. The product is in product factory default state.
- 1692 2. Documentation describing the legacy protocols supported by the product is available.

1693 **Assessment activities**

- 1694 1. Review documentation to list each legacy protocol supported by the product.
- 1695 2. Scan the product in product factory default state to enumerate network-accessible services. Verify that no
 1696 enabled network-accessible service relies on a legacy protocol.
- 1697 3. Scan the product in product factory default state to enumerate active protocols. Verify that each documented
 1698 legacy protocol is disabled.
- 1699 4. Attempt to activate each documented legacy protocol without performing the documented management action.
 1700 Verify that the legacy protocol remains disabled.

1701 **Assessment verdict**

1702 The verdict fail is assigned if any of the following conditions apply:

- 1703 1. Documentation does not list each legacy protocol supported by the product.
- 1704 2. The product enables a network-accessible service that relies on a legacy protocol in product factory default
 1705 state.
- 1706 3. Any documented legacy protocol is enabled in product factory default state.
- 1707 4. Any documented legacy protocol becomes enabled when activation is attempted without the documented
 1708 management action.

1709 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1710 1. Documentation lists each legacy protocol supported by the product.
- 1711 2. The product does not enable any network-accessible service that relies on a legacy protocol in product factory
 1712 default state.
- 1713 3. Each documented legacy protocol remains disabled in product factory default state.
- 1714 4. Each documented legacy protocol remains disabled when activation is attempted without the documented
 1715 management action.

1716 **Assessment evidence**

- 1717 1. Documentation listing each legacy protocol supported by the product.
- 1718 2. Test results showing no enabled network-accessible service relies on a legacy protocol in product factory
 1719 default state.
- 1720 3. Test results showing each documented legacy protocol is disabled in product factory default state.

- 1721 4. Test results showing each documented legacy protocol remains disabled when activation is attempted without
1722 the documented management action.
1723

1724 [\[AC-DEFAULT-1-10\]](#) Verify that the product provides a user-facing indication that the legacy protocol is in use, where
1725 the product has activated a legacy protocol it supports.

1726 **Assessment reference**

1727 Requirement [\[REQ-DEFAULT-1-10\]](#).

1728 **Assessment objective**

1729 Confirm that the product provides a user-facing indication that the legacy protocol is in use whenever a supported
1730 legacy protocol is active on the product.

1731 **Assessment preparation**

- 1732 1. The product is in product operational state.
1733 2. Documentation describing the legacy protocols supported by the product and the user-facing indication
1734 mechanism is available.

1735 **Assessment activities**

- 1736 1. Review documentation to identify the user-facing indication mechanism for each legacy protocol supported by
1737 the product.
1738 2. Enable each documented legacy protocol in turn using the documented management action. Verify that the
1739 product presents the user-facing indication that the legacy protocol is in use.

1740 **Assessment verdict**

1741 The verdict fail is assigned if any of the following conditions apply:

- 1742 1. Documentation does not describe the user-facing indication mechanism for any legacy protocol supported by
1743 the product.
1744 2. The product does not present a user-facing indication that the legacy protocol is in use for any enabled legacy
1745 protocol.

1746 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1747 1. Documentation describes the user-facing indication mechanism for each legacy protocol supported by the
1748 product.
1749 2. The product presents a user-facing indication that the legacy protocol is in use for each enabled legacy
1750 protocol.

1751 **Assessment evidence**

- 1752 1. Documentation describing the user-facing indication mechanism for each legacy protocol supported by the
1753 product.
1754 2. Test results showing the product presents a user-facing indication that the legacy protocol is in use for each
1755 enabled legacy protocol.
1756

1757 [\[AC-DEFAULT-1-11\]](#) Verify that the manufacturer records in the technical documentation referred to in Annex VII of
1758 Regulation (EU) 2024/2847, for each legacy protocol supported by the product, (i) the legacy protocol; (ii) the security
1759 features that are no longer considered state of the art; (iii) the specific legacy system or systems for which the protocol
1760 is required; and (iv) the constraint preventing the use of a state of the art alternative.

1761 **Assessment reference**

1762 Requirement [\[REQ-DEFAULT-1-11\]](#).

1763 **Assessment objective**

1764 Confirm that the technical documentation records, for each legacy protocol supported by the product, (i) the legacy
1765 protocol; (ii) the security features that are no longer considered state of the art; (iii) the specific legacy system or
1766 systems for which the protocol is required; and (iv) the constraint preventing the use of a state of the art alternative.

1767 **Assessment preparation**

- 1768 1. The product is in product operational state.
 1769 2. The technical documentation referred to in Annex VII of Regulation (EU) 2024/2847 is available.

1770 **Assessment activities**

- 1771 1. Review documentation to list each legacy protocol supported by the product.
 1772 2. Review documentation for the security features that are no longer considered state of the art for each
 1773 documented legacy protocol.
 1774 3. Review documentation for the legacy system or systems for which each documented legacy protocol is
 1775 required.
 1776 4. Review documentation for the constraint preventing the use of a state of the art alternative for each
 1777 documented legacy protocol.

1778 **Assessment verdict**

1779 The verdict fail is assigned if any of the following conditions apply:

- 1780 1. Documentation does not list each legacy protocol supported by the product.
 1781 2. Documentation does not list the security features that are no longer considered state of the art for any
 1782 documented legacy protocol.
 1783 3. Documentation does not list the legacy system or systems for any documented legacy protocol.
 1784 4. Documentation does not describe the constraint preventing the use of a state of the art alternative for any
 1785 documented legacy protocol.

1786 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1787 1. Documentation lists each legacy protocol supported by the product.
 1788 2. Documentation lists the security features that are no longer considered state of the art for each documented
 1789 legacy protocol.
 1790 3. Documentation lists the legacy system or systems for which each documented legacy protocol is required.
 1791 4. Documentation describes the constraint preventing the use of a state of the art alternative for each documented
 1792 legacy protocol.

1793 **Assessment evidence**

- 1794 1. Documentation listing each legacy protocol supported by the product.
 1795 2. Documentation listing the security features that are no longer considered state of the art for each documented
 1796 legacy protocol.
 1797 3. Documentation listing the legacy system or systems for which each documented legacy protocol is required.
 1798 4. Documentation describing the constraint preventing the use of a state of the art alternative for each
 1799 documented legacy protocol.
 1800

1801 [\[AC-DEFAULT-1-12\]](#) Verify that the product enforces the principle of least privilege during normal operation.

1802 **Assessment reference**

1803 Requirement [\[REQ-DEFAULT-1-12\]](#).

1804 **Assessment objective**

1805 Confirm that the product enforces the principle of least privilege by defining distinct privilege levels, restricting each
 1806 account to its assigned privileges, and preventing privilege escalation without authorization.

1807 **Assessment preparation**

- 1808 1. The product is in specific operational state with initialization complete.
 1809 2. Documentation describing the role and permission model is available.
 1810 3. Accounts for each defined role are available or can be created.

1811 **Assessment activities**

- 1812 1. Review documentation to identify all defined roles and their assigned operations.
 1813 2. Authenticate with an account of each defined role. Verify that all assigned operations are available.
 1814 3. Authenticate with each defined role in turn and attempt operations assigned to a higher-privilege role. Verify
 1815 that access is denied for each attempt.

- 1816 4. Attempt privilege escalation without authorization. Verify that the product rejects the attempt.
 1817 5. Inspect running processes and services on the product where accessible to verify they run with minimum
 1818 required privileges and not as root or equivalent unless documented as necessary.

1819 **Assessment verdict**

1820 The verdict fail is assigned if any of the following conditions apply:

- 1821 1. Documentation does not list all roles, their privilege levels, and assigned operations.
 1822 2. Any defined role does not perform all its assigned operations.
 1823 3. The product does not deny operations assigned to higher-privilege roles to lower-privilege accounts.
 1824 4. The product does not reject privilege escalation attempts without authorization.
 1825 5. The product does not run all inspected processes with minimum required privileges where process listing is
 1826 accessible.

1827 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1828 1. Documentation lists all roles, their privilege levels, and assigned operations.
 1829 2. Each defined role performs all its assigned operations.
 1830 3. The product denies operations assigned to higher-privilege roles to lower-privilege accounts.
 1831 4. The product rejects privilege escalation attempts without authorization.
 1832 5. The product runs all inspected processes with minimum required privileges where process listing is accessible.

1833 **Assessment evidence**

- 1834 1. Documentation listing all roles, privilege levels, and assigned operations.
 1835 2. Test results showing each defined role performs all its assigned operations.
 1836 3. Test results showing the product denies operations assigned to higher-privilege roles to lower-privilege
 1837 accounts.
 1838 4. Test results showing the product rejects privilege escalation attempts without authorization.
 1839 5. Test results showing the product runs all inspected processes with minimum required privileges where process
 1840 listing is accessible.
 1841

1842 [\[AC-DEFAULT-1-13\]](#) Verify that the product stores audit events in persistent memory that survives a reboot.

1843 **Assessment reference**

1844 Requirement [\[REQ-DEFAULT-1-13\]](#).

1845 **Assessment objective**

1846 Confirm that the product stores audit events in persistent memory that survives the reboot.

1847 **Assessment preparation**

- 1848 1. The product is in specific operational state.
 1849 2. Documentation describing audit event storage mechanisms is available.

1850 **Assessment activities**

- 1851 1. Review documentation to identify the audit event storage mechanism.
 1852 2. Perform a reboot. Verify that audit events recorded before the reboot are present and intact after the reboot.
 1853 3. Perform a power cycle. Verify that audit events recorded before the power cycle are present and intact after the
 1854 power cycle.

1855 **Assessment verdict**

1856 The verdict fail is assigned if any of the following conditions apply:

- 1857 1. Documentation does not list the audit event storage mechanism.
 1858 2. The product does not store audit events in persistent memory that survives a reboot.
 1859 3. The product does not store audit events in persistent memory that survives a power cycle.

1860 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1861 1. Documentation lists the audit event storage mechanism.

- 1862 2. The product stores audit events in persistent memory that survives a reboot.
 1863 3. The product stores audit events in persistent memory that survives a power cycle.

1864 **Assessment evidence**

- 1865 1. Documentation listing the audit event storage mechanism.
 1866 2. Test results showing the product stores audit events in persistent memory that survives a reboot.
 1867 3. Test results showing the product stores audit events in persistent memory that survives a power cycle.
 1868

1869 **6.3.2 [RESET-1] Factory reset**

1870 **6.3.2.1 Requirement assessments**

1871 [\[AC-RESET-1-01\]](#) Verify that the product provides a factory reset mechanism that restores the product to its secure-by-
 1872 default configuration.

1873 **Assessment reference**

1874 Requirement [\[REQ-RESET-1-01\]](#).

1875 **Assessment objective**

1876 Confirm that the product provides a factory reset mechanism that restores the product to its secure-by-default
 1877 configuration.

1878 **Assessment preparation**

- 1879 1. The product is in specific operational state.
 1880 2. Documentation describing the factory reset mechanism and procedure is available.

1881 **Assessment activities**

- 1882 1. Review documentation to identify the factory reset mechanism and procedure. Verify the product provides a
 1883 documented factory reset mechanism.
 1884 2. Perform a factory reset. Verify that the product is restored to its secure-by-default configuration.
 1885 3. Perform the assessments in clause [5.4.1](#) on the post-reset product. Verify that all assessments pass.

1886 **Assessment verdict**

1887 The verdict fail is assigned if any of the following conditions apply:

- 1888 1. Documentation does not describe the factory reset mechanism or procedure.
 1889 2. The product does not restore its secure-by-default configuration after factory reset.
 1890 3. The product does not pass all assessments in clause [5.4.1](#) after factory reset.

1891 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1892 1. Documentation describes the factory reset mechanism and procedure.
 1893 2. The product restores its secure-by-default configuration after factory reset.
 1894 3. The product passes all assessments in clause [5.4.1](#) after factory reset.

1895 **Assessment evidence**

- 1896 1. Documentation describing the factory reset mechanism and procedure.
 1897 2. Test results showing the product is restored to its secure-by-default configuration after factory reset.
 1898 3. Test results showing the product passes all assessments in clause [5.4.1](#) after factory reset.
 1899

1900 [\[AC-RESET-1-02\]](#) Verify that the product maintains the currently installed firmware version and all installed security
 1901 updates after factory reset.

1902 **Assessment reference**

1903 Requirement [\[REQ-RESET-1-02\]](#).

1904 **Assessment objective**

1905 Confirm that the product provides a factory reset mechanism that maintains the currently installed firmware version and
 1906 all installed security updates, without reverting to the firmware version when made available on the market.

1907 **Assessment preparation**

- 1908 1. The product is in specific operational state with at least one security update applied beyond the firmware
 1909 version when made available on the market.
 1910 2. Documentation describing factory reset behaviour for firmware version and security updates is available.

1911 **Assessment activities**

- 1912 1. Review documentation to confirm the product provides a factory reset mechanism that preserves firmware
 1913 version and security updates.
 1914 2. Perform factory reset. Verify that the product maintains (i) the currently installed firmware version; and (ii) all
 1915 installed security updates.

1916 **Assessment verdict**

1917 The verdict fail is assigned if any of the following conditions apply:

- 1918 1. Documentation does not describe that factory reset preserves firmware version and installed security updates.
 1919 2. The product does not maintain the currently installed firmware version after factory reset.
 1920 3. Any installed security update does not remain applied after factory reset.

1921 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1922 1. Documentation describes that factory reset preserves firmware version and installed security updates.
 1923 2. The product maintains the currently installed firmware version after factory reset.
 1924 3. All installed security updates remain applied after factory reset.

1925 **Assessment evidence**

- 1926 1. Documentation describing factory reset behaviour for firmware and installed security updates.
 1927 2. Test results showing the product maintains the currently installed firmware version after factory reset.
 1928 3. Test results showing all installed security updates remain applied after factory reset.
 1929

1930 [\[AC-RESET-1-03\]](#) Verify that the product does not retain (i) not-default configuration; (ii) user data; or (iii) user-
 1931 instantiated or modified critical security parameters after factory reset.

1932 **Assessment reference**

1933 Requirement [\[REQ-RESET-1-03\]](#).

1934 **Assessment objective**

1935 Confirm that the product does not retain (i) not-default configuration; (ii) user data; or (iii) user-instantiated or modified
 1936 critical security parameters after factory reset.

1937 **Assessment preparation**

- 1938 1. The product is in specific operational state.
 1939 2. Documentation describing factory reset behaviour is available.

1940 **Assessment activities**

- 1941 1. Review documentation to identify data retained and data removed during factory reset.
 1942 2. Modify the product configuration to a not-default state, create user data, and configure user-instantiated or
 1943 modified critical security parameters. Verify the modifications are present before factory reset.
 1944 3. Perform factory reset. Attempt to retrieve the previously modified configuration through the product.
 1945 4. Attempt to retrieve the previously created user data through the product after factory reset.
 1946 5. Attempt to retrieve the previously configured user-instantiated or modified critical security parameters through
 1947 the product after factory reset.

1948 **Assessment verdict**

1949 The verdict fail is assigned if any of the following conditions apply:

- 1950 1. Documentation does not describe data retained and data removed during factory reset.
- 1951 2. The product does not contain not-default configuration, user data, or user-instantiated or modified critical
- 1952 security parameters before factory reset.
- 1953 3. The product retains not-default configuration after factory reset.
- 1954 4. The product retains user data after factory reset.
- 1955 5. The product retains user-instantiated or modified critical security parameters after factory reset.

1956 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1957 1. Documentation describes data retained and data removed during factory reset.
- 1958 2. The product contains not-default configuration, user data, and user-instantiated or modified critical security
- 1959 parameters before factory reset.
- 1960 3. The product does not retain not-default configuration after factory reset.
- 1961 4. The product does not retain user data after factory reset.
- 1962 5. The product does not retain user-instantiated or modified critical security parameters after factory reset.

1963 **Assessment evidence**

- 1964 1. Documentation describing data retained and data removed during factory reset.
- 1965 2. Test results showing the product contains not-default configuration, user data, and user-instantiated or
- 1966 modified critical security parameters before factory reset.
- 1967 3. Test results showing the product does not retain not-default configuration after factory reset.
- 1968 4. Test results showing the product does not retain user data after factory reset.
- 1969 5. Test results showing the product does not retain user-instantiated or modified critical security parameters after
- 1970 factory reset.
- 1971

1972 **6.4 Security updates**

1973 **6.4.1 [UPDATE-1] Update mechanisms**

1974 **6.4.1.1 Requirement assessments**

1975 [\[AC-UPDATE-1-01\]](#) Verify that the product provides a mechanism to receive security updates.

1976 **Assessment reference**

1977 Requirement [\[REQ-UPDATE-1-01\]](#).

1978 **Assessment objective**

1979 Confirm that the product provides a mechanism to receive security updates through on-product delivery, off-the-product

1980 delivery, or both.

1981 **Assessment preparation**

- 1982 1. The product is in specific operational state.
- 1983 2. Documentation describing the security update delivery method is available.

1984 **Assessment activities**

- 1985 1. Review documentation to identify whether the product supports on-product delivery, off-the-product delivery,
- 1986 or both.
- 1987 2. For products not designed for configuration and maintenance by professional network administrators, verify
- 1988 that the product downloads the security update through the on-product mechanism, where the product supports
- 1989 on-product delivery.
- 1990 3. For products not designed for configuration and maintenance by professional network administrators, obtain a
- 1991 security update through the documented off-the-product procedure, where the product supports off-the-product
- 1992 delivery.

1993 **Assessment verdict**

1994 The verdict fail is assigned if any of the following conditions apply:

- 1995 1. Documentation does not describe the security update delivery method.

- 1996 2. The product does not download the security update through the on-product mechanism.
 1997 3. The product does not provide a mechanism to receive security updates through the documented off-the-product
 1998 procedure.

1999 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2000 1. Documentation describes the security update delivery method.
 2001 2. The product downloads the security update through the on-product mechanism.
 2002 3. The product provides a mechanism to receive security updates through the documented off-the-product
 2003 procedure.

2004 **Assessment evidence**

- 2005 1. Documentation describing the security update delivery method.
 2006 2. Test results showing the product downloads the security update through the on-product mechanism.
 2007 3. Test results showing the product provides a mechanism to receive security updates through the off-the-product
 2008 procedure.
 2009

2010 [\[AC-UPDATE-1-02\]](#) Verify that the product prevents installation of security updates without authentication and
 2011 authorization.

2012 **Assessment reference**

2013 Requirement [\[REQ-UPDATE-1-02\]](#).

2014 **Assessment objective**

2015 Confirm that the product prevents installation of security updates without authentication and authorization.

2016 **Assessment preparation**

- 2017 1. The product is in specific operational state.
 2018 2. For products not designed for configuration and maintenance by professional network administrators,
 2019 documentation describing authentication and authorization requirements for security update installation is
 2020 available.

2021 **Assessment activities**

- 2022 1. Review documentation to identify the authentication and authorization requirements for security update
 2023 installation.
 2024 2. Attempt to install a security update without authentication. Verify that the product prevents the installation.
 2025 3. Attempt to install a security update without authorization. Verify that the product prevents the installation.

2026 **Assessment verdict**

2027 The verdict fail is assigned if any of the following conditions apply:

- 2028 1. Documentation does not describe the authentication and authorization requirements for security update
 2029 installation.
 2030 2. For products not designed for configuration and maintenance by professional network administrators, the
 2031 product does not prevent security update installation without authentication.
 2032 3. The product does not prevent security update installation without authorization.

2033 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2034 1. Documentation describes the authentication and authorization requirements for security update installation.
 2035 2. For products not designed for configuration and maintenance by professional network administrators, the
 2036 product prevents security update installation without authentication.
 2037 3. The product prevents security update installation without authorization.

2038 **Assessment evidence**

- 2039 1. Documentation describing the authentication and authorization requirements for security update installation.
 2040 2. Test results showing the product prevents security update installation without authentication.
 2041 3. Test results showing the product prevents security update installation without authorization.
 2042

2043 [\[AC-UPDATE-1-03\]](#) Verify that the product installs a received security update and reports the installed version.

2044 **Assessment reference**

2045 Requirement [\[REQ-UPDATE-1-03\]](#).

2046 **Assessment objective**

2047 Confirm that the product installs a received security update and reports the installed version after installation.

2048 **Assessment preparation**

- 2049 1. The product is in specific operational state.
- 2050 2. A security update has been received through the documented delivery method.

2051 **Assessment activities**

- 2052 1. Review documentation to identify the security update installation procedure and the version reporting
2053 mechanism.
- 2054 2. Install the received security update. Verify that the product reports the installed version after installation.

2055 **Assessment verdict**

2056 The verdict fail is assigned if any of the following conditions apply:

- 2057 1. Documentation does not describe the security update installation procedure and the version reporting
2058 mechanism.
- 2059 2. The product does not install the security update.
- 2060 3. The product does not report the installed version.

2061 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2062 1. Documentation describes the security update installation procedure and the version reporting mechanism.
- 2063 2. The product installs the security update.
- 2064 3. The product reports the installed version.

2065 **Assessment evidence**

- 2066 1. Documentation describing the security update installation procedure and the version reporting mechanism.
 - 2067 2. Test results showing the product installs the security update.
 - 2068 3. Test results showing the product reports the installed version.
- 2069

2070 [\[AC-UPDATE-1-04\]](#) Verify that when the product is not designed for configuration and maintenance by professional
2071 network administrators, the product automatically checks for security remedy updates according to the documented
2072 default schedule. Otherwise, verify that the procedure for checking for security updates is included in the instructions to
2073 the user.

2074 **Assessment reference**

2075 Requirement [\[REQ-UPDATE-1-04\]](#).

2076 **Assessment objective**

2077 Confirm that when the product is not designed for configuration and maintenance by professional network
2078 administrators, the product automatically checks for security remedy updates according to the documented default
2079 schedule, and otherwise that the instructions to the user include the procedure for checking for security updates.

2080 **Assessment preparation**

- 2081 1. The product is in specific operational state.
- 2082 2. Documentation identifying whether the product is designed for configuration and maintenance by professional
2083 network administrators is available.
- 2084 3. For products not designed for configuration and maintenance by professional network administrators,
2085 documentation describing the default schedule for checking security remedy updates is available.
- 2086 4. For products designed for configuration and maintenance by professional network administrators, instructions
2087 to the user are available.

2088 **Assessment activities**

- 2089 1. Review documentation to identify whether the product is designed for configuration and maintenance by
2090 professional network administrators and to identify the applicable update checking information.
- 2091 2. Where the product is not designed for configuration and maintenance by professional network administrators,
2092 inspect the product in specific operational state and verify that it automatically checks for security remedy
2093 updates according to the documented default schedule.
- 2094 3. Where the product is designed for configuration and maintenance by professional network administrators,
2095 follow the documented procedure for checking for security updates and verify that the procedure enables
2096 checking for security updates.

2097 **Assessment verdict**

2098 The verdict fail is assigned if any of the following conditions apply:

- 2099 1. Documentation does not identify whether the product is designed for configuration and maintenance by
2100 professional network administrators.
- 2101 2. Documentation does not describe the default schedule for checking security remedy updates where the product
2102 is not designed for configuration and maintenance by professional network administrators.
- 2103 3. Instructions to the user do not describe the procedure for checking for security updates where the product is
2104 designed for configuration and maintenance by professional network administrators.
- 2105 4. The product does not check for security remedy updates automatically according to the documented default
2106 schedule where the product is not designed for configuration and maintenance by professional network
2107 administrators.
- 2108 5. The documented procedure does not enable checking for security updates where the product is designed for
2109 configuration and maintenance by professional network administrators.

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

- 2111 1. Documentation identifies whether the product is designed for configuration and maintenance by professional
2112 network administrators.
- 2113 2. Documentation describes the default schedule for checking security remedy updates where the product is not
2114 designed for configuration and maintenance by professional network administrators.
- 2115 3. Instructions to the user describe the procedure for checking for security updates where the product is designed
2116 for configuration and maintenance by professional network administrators.
- 2117 4. The product checks for security remedy updates automatically according to the documented default schedule
2118 where the product is not designed for configuration and maintenance by professional network administrators.
- 2119 5. The documented procedure enables checking for security updates where the product is designed for
2120 configuration and maintenance by professional network administrators.

2121 **Assessment evidence**

- 2122 1. Documentation identifying whether the product is designed for configuration and maintenance by professional
2123 network administrators.
- 2124 2. Documentation describing the default schedule for checking security remedy updates where the product is not
2125 designed for configuration and maintenance by professional network administrators.
- 2126 3. Instructions to the user describing the procedure for checking for security updates where the product is
2127 designed for configuration and maintenance by professional network administrators.
- 2128 4. Test results showing the product checks for security remedy updates automatically according to the
2129 documented default schedule where the product is not designed for configuration and maintenance by
2130 professional network administrators.
- 2131 5. Test results showing the documented procedure enables checking for security updates where the product is
2132 designed for configuration and maintenance by professional network administrators.
- 2133

2134 [\[AC-UPDATE-1-05\]](#) Verify that when the product is not designed for configuration and maintenance by professional
2135 network administrators, the security update mechanism is automated and enabled by default. Otherwise, verify that the
2136 procedure for performing the security update is included in the instructions to the user.

2137 **Assessment reference**

2138 Requirement [\[REQ-UPDATE-1-05\]](#).

2139 **Assessment objective**

2140 Confirm that when the product is not designed for configuration and maintenance by professional network
 2141 administrators, the security update mechanism is automated and enabled by default, and otherwise that the instructions
 2142 to the user include the procedure for performing the security update.

2143 **Assessment preparation**

- 2144 1. The product is in product factory default state.
- 2145 2. Documentation identifying whether the product is designed for configuration and maintenance by professional
 2146 network administrators is available.
- 2147 3. For products designed for configuration and maintenance by professional network administrators, instructions
 2148 to the user are available.
- 2149 4. A security update is available through the documented delivery method.

2150 **Assessment activities**

- 2151 1. Review documentation to identify whether the product is designed for configuration and maintenance by
 2152 professional network administrators and to identify the applicable security update mechanism or procedure.
- 2153 2. Where the product is not designed for configuration and maintenance by professional network administrators,
 2154 inspect the product in product factory default state and verify that the security update mechanism is automated
 2155 and enabled by default.
- 2156 3. Where the product is designed for configuration and maintenance by professional network administrators,
 2157 follow the documented procedure for performing the security update and verify that the procedure enables the
 2158 security update to be performed.

2159 **Assessment verdict**

2160 The verdict fail is assigned if any of the following conditions apply:

- 2161 1. Documentation does not identify whether the product is designed for configuration and maintenance by
 2162 professional network administrators.
- 2163 2. Documentation does not describe the automated and enabled-by-default security update mechanism where the
 2164 product is not designed for configuration and maintenance by professional network administrators.
- 2165 3. Instructions to the user do not describe the procedure for performing the security update where the product is
 2166 designed for configuration and maintenance by professional network administrators.
- 2167 4. The product does not provide a security update mechanism that is automated and enabled by default where the
 2168 product is not designed for configuration and maintenance by professional network administrators.
- 2169 5. The documented procedure does not enable the security update to be performed where the product is designed
 2170 for configuration and maintenance by professional network administrators.

2171 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2172 1. Documentation identifies whether the product is designed for configuration and maintenance by professional
 2173 network administrators.
- 2174 2. Documentation describes the automated and enabled-by-default security update mechanism where the product
 2175 is not designed for configuration and maintenance by professional network administrators.
- 2176 3. Instructions to the user describe the procedure for performing the security update where the product is
 2177 designed for configuration and maintenance by professional network administrators.
- 2178 4. The product provides a security update mechanism that is automated and enabled by default where the product
 2179 is not designed for configuration and maintenance by professional network administrators.
- 2180 5. The documented procedure enables the security update to be performed where the product is designed for
 2181 configuration and maintenance by professional network administrators.

2182 **Assessment evidence**

- 2183 1. Documentation identifying whether the product is designed for configuration and maintenance by professional
 2184 network administrators.
- 2185 2. Documentation describing the automated and enabled-by-default security update mechanism where the product
 2186 is not designed for configuration and maintenance by professional network administrators.
- 2187 3. Instructions to the user describing the procedure for performing the security update where the product is
 2188 designed for configuration and maintenance by professional network administrators.
- 2189 4. Test results showing the product provides a security update mechanism that is automated and enabled by
 2190 default where the product is not designed for configuration and maintenance by professional network
 2191 administrators.

- 2192 5. Test results showing the documented procedure enables the security update to be performed where the product
 2193 is designed for configuration and maintenance by professional network administrators.
 2194

2195 [\[AC-UPDATE-1-06\]](#) Verify that the product verifies security update integrity using state of the art cryptography before
 2196 installation.

2197 **Assessment reference**

2198 Requirement [\[REQ-UPDATE-1-06\]](#).

2199 **Assessment objective**

2200 Confirm that the product verifies security update integrity using state of the art cryptography before installation.

2201 **Assessment preparation**

- 2202 1. The product is in specific operational state.
 2203 2. Documentation describing the security update integrity verification mechanism is available.

2204 **Assessment activities**

- 2205 1. Review documentation to identify the security update integrity verification mechanism.
 2206 2. Inspect the documented security update verification mechanism. Verify the cryptography used is state of the
 2207 art.
 2208 3. Install a valid security update. Verify the product performs cryptographic verification before installation
 2209 proceeds.
 2210 4. Attempt to install a tampered security update. Verify that the product rejects the installation.

2211 **Assessment verdict**

2212 The verdict fail is assigned if any of the following conditions apply:

- 2213 1. Documentation does not describe the security update integrity verification mechanism.
 2214 2. The product does not use state of the art cryptography for security update verification.
 2215 3. The product does not perform cryptographic verification before installing the security update.
 2216 4. The product does not reject installation of a tampered security update.

2217 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2218 1. Documentation describes the security update integrity verification mechanism.
 2219 2. The product uses state of the art cryptography for security update verification.
 2220 3. The product performs cryptographic verification before installing the security update.
 2221 4. The product rejects installation of a tampered security update.

2222 **Assessment evidence**

- 2223 1. Documentation describing the security update integrity verification mechanism.
 2224 2. Test results showing the security update verification uses state of the art cryptography.
 2225 3. Test results showing the product performs cryptographic verification before installing the security update.
 2226 4. Test results showing the product rejects installation of a tampered security update.
 2227

2228 [\[AC-UPDATE-1-07\]](#) Verify that the product generates audit events for (i) security update availability; (ii) security
 2229 update download initiation, completion, or failure; and (iii) security update installation success or failure.

2230 **Assessment reference**

2231 Requirement [\[REQ-UPDATE-1-07\]](#).

2232 **Assessment objective**

2233 Confirm that the product generates audit events for (i) security update availability; (ii) security update download
 2234 initiation, completion, or failure; and (iii) security update installation success or failure.

2235 **Assessment preparation**

- 2236 1. The product is in specific operational state.

2237 2. Documentation describing audit events generated for security update activities is available.

2238 **Assessment activities**

- 2239 1. Review documentation to identify the audit events generated for security update activities.
 2240 2. Trigger a security update availability notification. Verify that the product generates an audit event for security
 2241 update availability.
 2242 3. Initiate and complete a security update download. Verify that the product generates audit events for security
 2243 update download initiation, completion, or failure.
 2244 4. Perform a security update installation. Verify that the product generates an audit event for security update
 2245 installation success or failure.

2246 **Assessment verdict**

2247 The verdict fail is assigned if any of the following conditions apply:

- 2248 1. Documentation does not describe audit events for security update activities.
 2249 2. The product does not generate an audit event for security update availability.
 2250 3. The product does not generate audit events for security update download initiation, completion, or failure.
 2251 4. The product does not generate an audit event for security update installation success or failure.

2252 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2253 1. Documentation describes audit events for security update activities.
 2254 2. The product generates an audit event for security update availability.
 2255 3. The product generates audit events for security update download initiation, completion, or failure.
 2256 4. The product generates an audit event for security update installation success or failure.

2257 **Assessment evidence**

- 2258 1. Documentation describing audit events generated for security update activities.
 2259 2. Test results showing the product generates an audit event for security update availability.
 2260 3. Test results showing the product generates audit events for security update download initiation, completion, or
 2261 failure.
 2262 4. Test results showing the product generates an audit event for security update installation success or failure.
 2263

2264 **6.5 Access control**

2265 **6.5.1 [AUTH-1] Authentication**

2266 **6.5.1.1 Requirement assessments**

2267 [\[AC-AUTH-1-01\]](#) Verify that the product requires user authentication on all interfaces providing management access to
 2268 the product.

2269 **Assessment reference**

2270 Requirement [\[REQ-AUTH-1-01\]](#).

2271 **Assessment objective**

2272 Confirm that the product requires user authentication on all interfaces providing management access to the product, and
 2273 that access without authentication is denied.

2274 **Assessment preparation**

- 2275 1. The product is in specific operational state.
 2276 2. Documentation describing the user authentication mechanism is available.

2277 **Assessment activities**

- 2278 1. Review documentation to identify all authentication mechanisms and management interfaces on which
 2279 authentication is required.
 2280 2. Attempt to access the product on each management interface without providing credentials. Verify access is
 2281 denied.

- 2282 3. Authenticate using valid credentials on each management interface. Verify access is granted.
 2283 4. Authenticate using valid credentials and perform a series of operations without re-authenticating. Verify the
 2284 product maintains authentication state throughout the session without requiring repeated credential entry.
 2285 5. Attempt to access the product on each management interface with invalid credentials. Verify access is denied.

2286 **Assessment verdict**

2287 The verdict fail is assigned if any of the following conditions apply:

- 2288 1. Documentation does not describe the authentication mechanism, method, or management interfaces requiring
 2289 authentication.
 2290 2. The product does not deny access without authentication on any management interface.
 2291 3. The product does not grant access with valid credentials on any management interface.
 2292 4. The product does not maintain authentication state throughout the session without requiring repeated credential
 2293 entry.
 2294 5. The product does not reject invalid credentials on any management interface.

2295 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2296 1. Documentation describes the authentication mechanism, method, and all management interfaces requiring
 2297 authentication.
 2298 2. The product denies access without authentication on all management interfaces.
 2299 3. The product grants access with valid credentials on each management interface.
 2300 4. The product maintains authentication state throughout the session without requiring repeated credential entry.
 2301 5. The product rejects invalid credentials on each management interface.

2302 **Assessment evidence**

- 2303 1. Documentation describing the authentication mechanism, method, and all management interfaces requiring
 2304 authentication.
 2305 2. Test results showing access without authentication is denied on each management interface.
 2306 3. Test results showing valid credentials grant access on each management interface.
 2307 4. Test results showing the product maintains authentication state throughout the session using valid credentials
 2308 without re-authenticating.
 2309 5. Test results showing the product rejects invalid credentials on each management interface.
 2310

2311 [\[AC-AUTH-1-02\]](#) Verify that the product eliminates shared default credentials by either (i) generating credentials
 2312 during secure production; (ii) enforcing mandatory credential creation during initial setup; or (iii) using non-password
 2313 based authentication credentials.

2314 **Assessment reference**

2315 Requirement [\[REQ-AUTH-1-02\]](#).

2316 **Assessment objective**

2317 Confirm that the product eliminates shared default credentials by either (i) generating credentials during secure
 2318 production; (ii) enforcing mandatory credential creation during initial setup; or (iii) using non-password based
 2319 authentication credentials, and that no two product units share default credentials.

2320 **Assessment preparation**

- 2321 1. The product is in product factory default state.
 2322 2. Documentation describing the credential provisioning approach is available.

2323 **Assessment activities**

- 2324 1. Review documentation to identify whether credentials are provisioned by per-unit production generation, by
 2325 mandatory setup-time change, or by using non-password based authentication credentials.
 2326 2. When the product uses password-based credentials, compare factory default credentials across at least two
 2327 product units where production-generated credentials are used. Verify credentials differ across units and that
 2328 per-unit credentials are documented per device.

- 2329 3. When the product uses password-based credentials, start the initial setup process where setup-enforced
 2330 credentials are used. Verify mandatory credential creation is enforced before access is granted and that
 2331 credential creation cannot be skipped.
- 2332 4. When the product uses password-based credentials, verify the product does not allow normal operation with
 2333 shared default credentials.

2334 **Assessment verdict**

2335 The verdict fail is assigned if any of the following conditions apply:

- 2336 1. Documentation does not identify whether credentials are provisioned by per-unit production generation or by
 2337 mandatory setup-time change.
- 2338 2. Where production-generated credentials are used, two product units share identical default credentials.
- 2339 3. Where setup-enforced credentials are used, the product does not enforce mandatory credential creation before
 2340 granting access.
- 2341 4. Where setup-enforced credentials are used, the product permits the mandatory credential creation step to be
 2342 skipped.
- 2343 5. The product operates with shared default credentials.

2344 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2345 1. Documentation identifies whether credentials are provisioned by per-unit production generation or by
 2346 mandatory setup-time change.
- 2347 2. Where production-generated credentials are used, per-unit credentials differ across product units.
- 2348 3. Where setup-enforced credentials are used, the product enforces mandatory credential creation before access is
 2349 granted.
- 2350 4. Where setup-enforced credentials are used, the product does not permit the mandatory credential creation step
 2351 to be skipped.
- 2352 5. The product does not operate with shared default credentials.

2353 **Assessment evidence**

- 2354 1. Documentation describing whether credentials are provisioned by per-unit production generation or by
 2355 mandatory setup-time change, or documentation identifying that the product does not use password-based
 2356 credentials.
- 2357 2. Test results confirming credentials differ between product units where production-generated.
- 2358 3. Test results showing mandatory credential creation is enforced before access is granted where setup-enforced.
- 2359 4. Test results showing credential creation cannot be skipped.
- 2360 5. Test results confirming shared default credentials do not provide access.

2362 [\[AC-AUTH-1-03\]](#) Verify that where the product transmits critical security parameters, the product protects their
 2363 transmission over a secure channel and prevents disclosure of critical security parameters over an unencrypted channel.

2364 **Assessment reference**

2365 Requirement [\[REQ-AUTH-1-03\]](#).

2366 **Assessment objective**

2367 Confirm that where the product transmits critical security parameters, the product protects their transmission over a
 2368 secure channel and prevents disclosure of critical security parameters over an unencrypted channel.

2369 **Assessment preparation**

- 2370 1. The product is in specific operational state.
- 2371 2. Documentation describing the critical security parameter transmission mechanism and secure channel is
 2372 available.

2373 **Assessment activities**

- 2374 1. Review documentation to identify the secure channel used for critical security parameter transmission.
- 2375 2. Capture network traffic during an authentication attempt on each interface that accepts critical security
 2376 parameters. Verify the product transmits critical security parameters over a secure channel.

- 2377 3. Attempt to force critical security parameter transmission over an unencrypted channel. Verify that the product
2378 prevents disclosure of critical security parameters.

2379 **Assessment verdict**

2380 The verdict fail is assigned if any of the following conditions apply:

- 2381 1. Documentation does not describe the secure channel used for critical security parameter transmission.
2382 2. The product does not protect critical security parameters over a secure channel on any interface.
2383 3. The product does not prevent disclosure of critical security parameters over an unencrypted channel.

2384 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2385 1. Documentation describes the secure channel used for critical security parameter transmission.
2386 2. The product protects critical security parameters over a secure channel on all interfaces.
2387 3. The product prevents disclosure of critical security parameters over an unencrypted channel.

2388 **Assessment evidence**

- 2389 1. Documentation describing the secure channel used for critical security parameter transmission.
2390 2. Test results showing the product protects critical security parameters over a secure channel when transmitting
2391 on all interfaces.
2392 3. Test results showing the product prevents disclosure of critical security parameters when an unencrypted
2393 channel is forced.
2394

2395 [\[AC-AUTH-1-04\]](#) Verify that the product protects critical security parameters using state of the art cryptography.

2396 **Assessment reference**

2397 Requirement [\[REQ-AUTH-1-04\]](#).

2398 **Assessment objective**

2399 Confirm that the product protects critical security parameters using state of the art cryptography.

2400 **Assessment preparation**

- 2401 1. The product is in specific operational state with at least one user account configured.
2402 2. Documentation describing the critical security parameter storage mechanism is available.

2403 **Assessment activities**

- 2404 1. Review documentation to identify the cryptographic method used for critical security parameter storage and its
2405 parameters. Verify the documented method is state of the art.
2406 2. Inspect stored critical security parameters where storage is accessible, verifying they are not in plaintext and
2407 that a known-credential stored representation is consistent with the documented method. Inspect manufacturer
2408 technical documentation or source code where direct storage access is not available to confirm the
2409 implementation matches the documented method.
2410 3. Attempt to retrieve critical security parameters in plaintext through available interfaces without required
2411 authorization. Verify the product protects critical security parameters by denying retrieval.

2412 **Assessment verdict**

2413 The verdict fail is assigned if any of the following conditions apply:

- 2414 1. Documentation does not describe the critical security parameter storage method.
2415 2. The product does not use a state of the art critical security parameter storage method.
2416 3. The product stores critical security parameters in plaintext.
2417 4. The product does not store critical security parameters consistently with the documented method.
2418 5. The product permits retrieval of critical security parameters in plaintext without authorization.

2419 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2420 1. Documentation describes the critical security parameter storage method.
2421 2. The product uses a state of the art critical security parameter storage method.
2422 3. The product does not store critical security parameters in plaintext.
2423 4. The product stores critical security parameters consistently with the documented method.

2424 5. The product does not permit retrieval of critical security parameters in plaintext without authorization.

2425 **Assessment evidence**

- 2426 1. Documentation describing the critical security parameter storage method, parameters, and standard reference.
- 2427 2. Test results showing the storage method is state of the art.
- 2428 3. Test results showing critical security parameters are not stored in plaintext, where direct access is available.
- 2429 4. Test results showing stored representation matches the documented method.
- 2430 5. Test results showing the implementation matches the documented storage method, where direct storage access
- 2431 is not available.
- 2432 6. Test results showing critical security parameters cannot be retrieved in plaintext without authorization.
- 2433

2434 [\[AC-AUTH-1-05\]](#) When supporting password-based credentials, verify that the product enforces minimum credential
2435 entropy.

2436 **Assessment reference**

2437 Requirement [\[REQ-AUTH-1-05\]](#).

2438 **Assessment objective**

2439 When supporting password-based credentials, confirm that the product enforces minimum credential entropy, for
2440 example through minimum length and character complexity requirements sufficient to ensure entropy, and rejects
2441 credentials that do not meet these requirements.

2442 **Assessment preparation**

- 2443 1. The product is in specific operational state.
- 2444 2. Documentation describing minimum credential entropy requirements is available.

2445 **Assessment activities**

- 2446 1. Review documentation to identify the minimum credential entropy requirements.
- 2447 2. Attempt to create or change a credential that does not meet the documented minimum entropy. Verify the
2448 product rejects the credential.
- 2449 3. Create or change a credential that meets the minimum entropy. Verify the product accepts it.

2450 **Assessment verdict**

2451 The verdict fail is assigned if any of the following conditions apply:

- 2452 1. Documentation does not describe the minimum credential entropy requirements.
- 2453 2. The product does not reject credentials that do not meet the minimum entropy.
- 2454 3. The product does not accept credentials meeting the minimum entropy.

2455 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2456 1. Documentation describes the minimum credential entropy requirements.
- 2457 2. The product rejects credentials that do not meet the minimum entropy.
- 2458 3. The product accepts credentials meeting the minimum entropy.

2459 **Assessment evidence**

- 2460 1. Documentation describing the minimum credential entropy requirements.
- 2461 2. Test results showing credentials that do not meet the minimum entropy are rejected.
- 2462 3. Test results showing credentials meeting the minimum entropy are accepted.
- 2463

2464 [\[AC-AUTH-1-06\]](#) Verify that the product enforces authentication failure protection by (i) progressive delays between
2465 failed attempts; and (ii) temporary account lockout after a configurable number of failed attempts.

2466 **Assessment reference**

2467 Requirement [\[REQ-AUTH-1-06\]](#).

2468 **Assessment objective**

2469 Confirm that the product enforces authentication failure protection by (i) progressive delays between failed attempts;
 2470 and (ii) temporary account lockout after a configurable number of failed attempts, and that both mechanisms are
 2471 documented with specific thresholds and durations.

2472 **Assessment preparation**

- 2473 1. The product is in specific operational state with at least one user account.
- 2474 2. Documentation describing the authentication failure protection mechanisms is available.

2475 **Assessment activities**

- 2476 1. Review documentation to identify the authentication failure protection parameters.
- 2477 2. Perform consecutive failed authentication attempts using invalid credentials and measure the delay between
 2478 allowed attempts. Verify the delay increases progressively with consecutive failures.
- 2479 3. Reset the authentication failure counter by successfully authenticating, then perform consecutive failed
 2480 attempts from a clean zero-failure state until the documented lockout threshold is reached. Verify the account
 2481 is temporarily locked and the lockout duration matches the documented value.
- 2482 4. Wait for lockout to expire and authenticate with valid credentials. Verify access is granted and failure counters
 2483 are reset.

2484 **Assessment verdict**

2485 The verdict fail is assigned if any of the following conditions apply:

- 2486 1. Documentation does not describe authentication failure protection mechanisms.
- 2487 2. Documentation does not list lockout threshold and duration values.
- 2488 3. The product does not apply a delay between consecutive failed authentication attempts.
- 2489 4. The product does not increase the delay with each consecutive failure.
- 2490 5. The product does not lock the account after consecutive failed authentication attempts reach the documented
 2491 lockout threshold.
- 2492 6. The product does not enforce the documented lockout duration.
- 2493 7. The product does not restore access with valid credentials after lockout expires.
- 2494 8. The product does not reset the failure counter after successful authentication following lockout.

2495 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2496 1. Documentation describes authentication failure protection mechanisms.
- 2497 2. Documentation lists lockout threshold and duration values.
- 2498 3. The product applies a delay between consecutive failed authentication attempts.
- 2499 4. The product increases the delay with each consecutive failure.
- 2500 5. The product locks the account after consecutive failed authentication attempts reach the documented lockout
 2501 threshold.
- 2502 6. The product enforces the documented lockout duration.
- 2503 7. The product restores access with valid credentials after lockout expires.
- 2504 8. The product resets the failure counter after successful authentication following lockout.

2505 **Assessment evidence**

- 2506 1. Documentation describing authentication failure protection mechanisms.
- 2507 2. Documentation listing lockout threshold and duration values.
- 2508 3. Test results showing the product applies progressive delays between consecutive failed authentication
 2509 attempts.
- 2510 4. Test results showing the delay increases with each consecutive failure.
- 2511 5. Test results from resetting the failure counter and performing consecutive failed authentication attempts
 2512 showing the product locks the account after the documented lockout threshold is reached.
- 2513 6. Test results showing the product enforces the documented lockout duration.
- 2514 7. Test results showing the product restores access with valid credentials after lockout expires.
- 2515 8. Test results showing the product resets the failure counter after successful authentication following lockout.
- 2516

2517 [\[AC-AUTH-1-07\]](#) Verify that the product supports maintaining the history of previously used passwords, in their
 2518 processed form, to prevent reuse, with a minimum of one previous password kept, and that password changes are
 2519 validated against this history before acceptance.

2520 **Assessment reference**

2521 Requirement [\[REQ-AUTH-1-07\]](#).

2522 **Assessment objective**

2523 Confirm that the product supports maintaining the history of previously used passwords in their processed form, retains
 2524 at least one previous password, and rejects password changes that attempt to reuse a password present in the history.

2525 **Assessment preparation**

- 2526 1. The product is in specific operational state with at least one user account.
 2527 2. Documentation describing the password history mechanism is available.

2528 **Assessment activities**

- 2529 1. Review documentation to identify the number of previous passwords retained and the storage form or
 2530 documentation to enable the user configuration of password history limit.
 2531 2. Review documentation to identify the password history depth and the cryptographic method used for storage.
 2532 3. Verify the documented password history depth meets the graduated minimum for the applicable risk factors.
 2533 4. Use the password change interface to (i) set a known password; (ii) change it to a different value; and (iii)
 2534 attempt to change it back to the original value. Verify the product rejects the change and informs the user that
 2535 the password is already present in the password history.
 2536 5. Change the password to a value that is not present in the password history. Verify the change is accepted.
 2537 6. Inspect the password history where storage is accessible. Verify previous passwords are stored using state of
 2538 the art cryptography, not in plaintext.
 2539 7. Test password history isolation across accounts by (i) configuring two separate user accounts; (ii) changing the
 2540 password on one account; and (iii) attempting to reuse that same password on the other account. Verify the
 2541 history of one account does not affect password validation on the other.

2542 **Assessment verdict**

2543 The verdict fail is assigned if any of the following conditions apply:

- 2544 1. Documentation does not describe the number of previous passwords retained or the storage form.
 2545 2. Documentation does not describe the password history mechanism or cryptographic storage method.
 2546 3. The product does not store the graduated minimum number of previous passwords for the applicable risk level.
 2547 4. The product does not reject password changes to passwords present in the history.
 2548 5. The product does not inform the user of the rejection reason.
 2549 6. The product does not accept new passwords not present in the history.
 2550 7. The product does not store password history using state of the art cryptography.
 2551 8. The product does not isolate password history across accounts.

2552 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2553 1. Documentation describes the number of previous passwords retained and the storage form.
 2554 2. Documentation describes the password history mechanism and cryptographic storage method.
 2555 3. The product stores the graduated minimum number of previous passwords for the applicable risk level.
 2556 4. The product rejects password changes to passwords present in the history.
 2557 5. The product informs the user of the rejection reason.
 2558 6. The product accepts new passwords not present in the history.
 2559 7. The product stores password history using state of the art cryptography.
 2560 8. The product isolates password history across accounts.

2561 **Assessment evidence**

- 2562 1. Documentation describing the number of previous passwords retained and the storage form.
 2563 2. Documentation describing the password history mechanism, depth, and cryptographic storage method.
 2564 3. Test results showing the product stores the graduated minimum number of previous passwords for the
 2565 applicable risk level.

- 2566 4. Test results showing passwords present in the password history are rejected.
 2567 5. Test results showing the user is informed of the rejection reason.
 2568 6. Test results showing new passwords not present in history are accepted.
 2569 7. Test results showing the product stores password history using state of the art cryptography.
 2570 8. Test results showing the product isolates password history across accounts.
 2571

2572 6.5.2 [AUTH-2] Authorization

2573 6.5.2.1 Requirement assessments

2574 [\[AC-AUTH-2-01\]](#) Verify that where the product supports more than one privilege level, the product enforces privilege
 2575 separation.

2576 **Assessment reference**

2577 Requirement [\[REQ-AUTH-2-01\]](#).

2578 **Assessment objective**

2579 Confirm that where the product supports more than one privilege level, the product enforces privilege separation.

2580 **Assessment preparation**

- 2581 1. The product is in specific operational state.
 2582 2. Documentation describing the privilege levels is available, where the product supports more than one privilege
 2583 level.

2584 **Assessment activities**

- 2585 1. Review documentation to identify whether the product supports more than one privilege level. Verify that the
 2586 documentation describes all privilege levels and the authentication mechanism for management access, where
 2587 applicable.
 2588 2. Attempt to access management functions without authentication, where the product supports more than one
 2589 privilege level. Verify access is denied.
 2590 3. Authenticate with non-management credentials and attempt to access management functions, where the
 2591 product supports more than one privilege level. Verify access is denied.
 2592 4. Authenticate with management credentials, where the product supports more than one privilege level. Verify
 2593 management functions are accessible.

2594 **Assessment verdict**

2595 The verdict fail is assigned if any of the following conditions apply:

- 2596 1. Documentation does not describe all supported privilege levels or the authentication mechanism for
 2597 management access.
 2598 2. The product does not deny access without authentication to management functions.
 2599 3. The product grants management access with non-management credentials.
 2600 4. The product does not grant access to management functions with management credentials.

2601 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2602 1. Documentation describes all supported privilege levels and the authentication mechanism for management
 2603 access.
 2604 2. The product denies access without authentication to management functions.
 2605 3. The product does not grant management access with non-management credentials.
 2606 4. The product grants access to management functions with management credentials.

2607 **Assessment evidence**

- 2608 1. Documentation describing all supported privilege levels and the authentication mechanism for management
 2609 access.
 2610 2. Test results showing management access attempts without authentication are denied.
 2611 3. Test results showing non-management credentials cannot access management functions.
 2612 4. Test results showing management credentials grant access to management functions.

2613

2614 [\[AC-AUTH-2-02\]](#) Verify that the product restricts each user to their authorized privilege level.

2615 **Assessment reference**

2616 Requirement [\[REQ-AUTH-2-02\]](#).

2617 **Assessment objective**

2618 Confirm that the product restricts each user to their authorized privilege level.

2619 **Assessment preparation**

2620 1. The product is in specific operational state.

2621 2. Documentation describing all privilege levels and the operations assigned to each level is available.

2622 **Assessment activities**

2623 1. Review documentation to identify all privilege levels and the operations assigned to each.

2624 2. Authenticate with an account at each privilege level and attempt all documented operations for that level.

2625 Verify they succeed.

2626 3. Authenticate with an account at each defined privilege level in turn and attempt operations assigned to a higher
2627 privilege level. Verify each attempt is denied.

2628 **Assessment verdict**

2629 The verdict fail is assigned if any of the following conditions apply:

2630 1. Documentation does not describe all privilege levels.

2631 2. Documentation does not describe the operations assigned to each privilege level.

2632 3. The product does not permit each user to perform all operations within their assigned privilege level.

2633 4. The product does not restrict users from performing operations above their assigned privilege level.

2634 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

2635 1. Documentation describes all privilege levels.

2636 2. Documentation describes the operations assigned to each privilege level.

2637 3. The product permits each user to perform all operations within their assigned privilege level.

2638 4. The product restricts users from performing operations above their assigned privilege level.

2639 **Assessment evidence**

2640 1. Documentation describing all privilege levels.

2641 2. Documentation describing the operations assigned to each privilege level.

2642 3. Test results showing the product permits each user to perform all operations within their assigned privilege
2643 level.

2644 4. Test results showing the product restricts users from performing operations above their assigned privilege
2645 level.

2646

2647 [\[AC-AUTH-2-03\]](#) Verify that the product enforces authorization control on all interfaces providing management access
2648 to the product.

2649 **Assessment reference**

2650 Requirement [\[REQ-AUTH-2-03\]](#).

2651 **Assessment objective**

2652 Confirm that the product enforces authorization control on all interfaces providing management access to the product.

2653 **Assessment preparation**

2654 1. The product is in specific operational state.

2655 2. Documentation listing all interfaces providing management access to the product and the access control
2656 mechanisms on each is available.

2657 **Assessment activities**

- 2658 1. Review documentation to identify all interfaces providing management access to the product and the access
2659 control mechanism on each.
- 2660 2. Attempt access on each interface providing management access to the product. Verify that the product enforces
2661 access control on each interface.

2662 **Assessment verdict**

2663 The verdict fail is assigned if any of the following conditions apply:

- 2664 1. Documentation does not describe all interfaces providing management access to the product and their access
2665 control mechanisms.
- 2666 2. The product does not enforce access control on any interface providing management access to the product.

2667 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2668 1. Documentation describes all interfaces providing management access to the product and their access control
2669 mechanisms.
- 2670 2. The product enforces access control on each interface providing management access to the product.

2671 **Assessment evidence**

- 2672 1. Documentation describing all interfaces providing management access to the product and the access control
2673 mechanism for each.
- 2674 2. Test results showing the product enforces access control on each interface providing management access to the
2675 product.
- 2676

2677 [\[AC-AUTH-2-04\]](#) Verify that the product denies execution of any command that is not authorized for the privilege level
2678 of the user issuing it.

2679 **Assessment reference**

2680 Requirement [\[REQ-AUTH-2-04\]](#).

2681 **Assessment objective**

2682 Confirm that the product denies execution of any command that is not authorized for the privilege level of the user
2683 issuing it.

2684 **Assessment preparation**

- 2685 1. The product is in specific operational state.
- 2686 2. Documentation describing the command authorization mechanism is available.

2687 **Assessment activities**

- 2688 1. Review documentation to identify the command authorization mechanism and the privilege level required for
2689 each command category.
- 2690 2. Authenticate with a lower-privilege account and attempt to execute commands from each higher-privilege
2691 category. Verify each is denied before execution.
- 2692 3. Authenticate with an authorized account and execute commands from the authorized category. Verify they
2693 succeed.
- 2694 4. Attempt to bypass command authorization by modifying command parameters or injecting commands through
2695 alternative input paths. Verify the product denies execution.

2696 **Assessment verdict**

2697 The verdict fail is assigned if any of the following conditions apply:

- 2698 1. Documentation does not describe the command authorization mechanism or privilege requirements per
2699 command category.
- 2700 2. The product does not validate privilege levels before command execution.
- 2701 3. The product does not reject higher-privilege commands from lower-privilege users.
- 2702 4. The product does not execute authorized commands successfully.
- 2703 5. The product does not deny execution when command parameters are modified or commands are injected
2704 through alternative input paths.

- 2705 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
- 2706 1. Documentation describes the command authorization mechanism and privilege requirements per command
- 2707 category.
- 2708 2. The product validates privilege levels before command execution.
- 2709 3. The product rejects higher-privilege commands from lower-privilege users.
- 2710 4. The product executes authorized commands successfully.
- 2711 5. The product denies execution when command parameters are modified or commands are injected through
- 2712 alternative input paths.

2713 **Assessment evidence**

- 2714 1. Documentation describing the command authorization mechanism and privilege requirements per command
- 2715 category.
- 2716 2. Test results showing the product validates privilege levels before command execution.
- 2717 3. Test results showing the product rejects higher-privilege commands from lower-privilege users.
- 2718 4. Test results showing authorized commands execute successfully for authorized accounts.
- 2719 5. Test results showing the product denies execution when command parameters are modified or commands are
- 2720 injected through alternative input paths.
- 2721

2722 **6.5.3 [AUTH-3] Authenticated session lifecycle**

2723 **6.5.3.1 Requirement assessments**

2724 [\[AC-AUTH-3-01\]](#) Verify that the product generates cryptographically secure management session identifiers using state

2725 of the art cryptography that are unique, non-predictable, and resistant to brute force attacks.

2726 **Assessment reference**

2727 Requirement [\[REQ-AUTH-3-01\]](#).

2728 **Assessment objective**

2729 Confirm that the product generates cryptographically secure management session identifiers using state of the art

2730 cryptography that are unique, non-predictable, and resistant to brute force attacks, using state of the art cryptography.

2731 **Assessment preparation**

- 2732 1. The product is in specific operational state with at least one authenticated session-capable interface.
- 2733 2. Documentation describing the session identifier generation mechanism is available.
- 2734 3. Documentation describing maximum concurrent sessions supported.

2735 **Assessment activities**

- 2736 1. Review documentation to identify the session identifier generation mechanism. Verify the documented session
- 2737 identifier generation mechanism is state of the art.
- 2738 2. Establish a number of concurrent sessions, where the number established is the minimum of 10 and the
- 2739 documented maximum number of concurrent sessions supported by the product. Verify that each session
- 2740 identifier is distinct.
- 2741 3. Test session identifier invalidation by (i) establishing an authenticated session and recording the identifier; (ii)
- 2742 invalidating the session; and (iii) immediately attempting to reuse the recorded identifier. Verify the product
- 2743 rejects the reused identifier.
- 2744 4. Attempt to authenticate using a fabricated session identifier. Verify the product rejects it.

2745 **Assessment verdict**

- 2746 The verdict fail is assigned if any of the following conditions apply:
- 2747 1. Documentation does not describe the session identifier generation mechanism.
- 2748 2. The product does not use a state of the art session identifier generation mechanism.
- 2749 3. Any concurrent session identifier is not distinct.
- 2750 4. The product does not reject a reused session identifier immediately after invalidation of an authenticated
- 2751 session.
- 2752 5. The product does not reject fabricated session identifiers.

2753 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2754 1. Documentation describes the session identifier generation mechanism.
- 2755 2. The product uses a state of the art session identifier generation mechanism.
- 2756 3. All concurrent session identifiers are distinct.
- 2757 4. The product rejects a reused session identifier immediately after invalidation of an authenticated session.
- 2758 5. The product rejects fabricated session identifiers.

2759 **Assessment evidence**

- 2760 1. Documentation describing the session identifier generation mechanism.
- 2761 2. Test results showing the session identifier generation mechanism is state of the art.
- 2762 3. Test results showing all concurrent session identifiers are distinct.
- 2763 4. Test results showing the product rejects a reused session identifier immediately after invalidation of an authenticated session.
- 2764 5. Test results showing fabricated session identifiers are rejected.

2766

2767 [\[AC-AUTH-3-02\]](#) Verify that the product enforces session timeout with configurable idle timeout periods and default
2768 values.

2769 **Assessment reference**

2770 Requirement [\[REQ-AUTH-3-02\]](#).

2771 **Assessment objective**

2772 Confirm that the product enforces session timeout with configurable idle timeout periods and default values.

2773 **Assessment preparation**

- 2774 1. The product is in specific operational state with at least one authenticated session.
- 2775 2. Documentation describing session timeout mechanisms, default timeout values, and configuration options is
2776 available.

2777 **Assessment activities**

- 2778 1. Review documentation to identify the default idle timeout value and the configurable range.
- 2779 2. Retrieve the default idle timeout value from documentation or product configuration and leave an authenticated
2780 session idle for that timeout period. Verify that the product terminates the session and requires re-
2781 authentication.
- 2782 3. Establish a new session and perform an operation during the timeout period. Verify the timeout counter resets
2783 and the session remains active.
- 2784 4. Configure the timeout period to a shorter value. Verify that the session terminates after the new period.
- 2785 5. Attempt to reuse a timed-out session. Verify that the product denies access.

2786 **Assessment verdict**

2787 The verdict fail is assigned if any of the following conditions apply:

- 2788 1. Documentation does not describe the default idle timeout value and configurable range.
- 2789 2. The product does not terminate sessions after the default idle timeout period.
- 2790 3. The product does not require re-authentication after session termination by idle timeout.
- 2791 4. The product does not reset the timeout counter when user activity occurs, or the session does not remain active.
- 2792 5. The product does not enforce configurable timeout periods.
- 2793 6. The product does not apply newly configured timeout values.
- 2794 7. The product does not deny access when a timed-out session is reused.

2795 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2796 1. Documentation describes the default idle timeout value and configurable range.
- 2797 2. The product terminates sessions after the default idle timeout period.
- 2798 3. The product requires re-authentication after session termination by idle timeout.
- 2799 4. The product resets the timeout counter when user activity occurs and the session remains active.
- 2800 5. The product enforces configurable timeout periods.

- 2801 6. The product applies newly configured timeout values.
 2802 7. The product denies access when a timed-out session is reused.

2803 **Assessment evidence**

- 2804 1. Documentation describing the session timeout mechanism, default idle timeout value, and configurable range.
 2805 2. Test results showing the product terminates sessions after the default idle timeout period.
 2806 3. Test results showing the product requires re-authentication after session termination by idle timeout.
 2807 4. Test results showing the timeout counter resets on user activity and the session remains active.
 2808 5. Test results showing the product enforces configurable timeout periods.
 2809 6. Test results showing the product applies newly configured timeout values.
 2810 7. Test results showing access is denied when a timed-out session is reused.
 2811

2812 [\[AC-AUTH-3-03\]](#) Verify that the product invalidates sessions immediately upon (i) user-initiated logout; (ii) timeout
 2813 expiration; (iii) authentication credential change; (iv) expiry of a credential's validity; or (v) management termination,
 2814 and that session invalidation securely removes all session data.

2815 **Assessment reference**

2816 Requirement [\[REQ-AUTH-3-03\]](#).

2817 **Assessment objective**

2818 Confirm that the product invalidates sessions immediately upon (i) user-initiated logout; (ii) timeout expiration; (iii)
 2819 authentication credential change; (iv) expiry of a credential's validity; or (v) management termination, that session
 2820 invalidation securely removes all session data, and that invalidated sessions cannot be reused.

2821 **Assessment preparation**

- 2822 1. The product is in specific operational state with at least one authenticated session.
 2823 2. Documentation describing session invalidation triggers and data removal mechanisms is available.

2824 **Assessment activities**

- 2825 1. Review documentation to identify all session invalidation triggers and data removal mechanisms.
 2826 2. Establish an authenticated session and perform a logout. Establish a second session and terminate it through
 2827 the management interface. Verify that the product denies access when either session identifier is reused.
 2828 3. Establish a session and change the authentication credential for the account. Verify that the product invalidates
 2829 the existing session and requires re-authentication.
 2830 4. Allow an established session to time out. Verify that the product denies access when the session identifier is
 2831 reused.
 2832 5. Trigger each session invalidation type in sequence and time each invalidation from trigger event to denial of
 2833 the session identifier. Verify no observable delay occurs.

2834 **Assessment verdict**

2835 The verdict fail is assigned if any of the following conditions apply:

- 2836 1. Documentation does not describe all invalidation triggers and data removal mechanisms.
 2837 2. The product does not invalidate sessions upon logout or termination.
 2838 3. The product does not reject invalidated session identifiers on subsequent use.
 2839 4. The product does not invalidate sessions upon authentication credential change.
 2840 5. The product does not invalidate sessions upon timeout expiration.
 2841 6. The product does not invalidate sessions without observable delay for all triggers.

2842 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2843 1. Documentation describes all invalidation triggers and data removal mechanisms.
 2844 2. The product invalidates sessions upon logout or termination.
 2845 3. The product rejects invalidated session identifiers on subsequent use.
 2846 4. The product invalidates sessions upon authentication credential change.
 2847 5. The product invalidates sessions upon timeout expiration.
 2848 6. The product invalidates sessions without observable delay for all triggers.

2849 Assessment evidence

- 2850 1. Documentation describing all session invalidation triggers and data removal mechanisms.
- 2851 2. Test results showing the product invalidates sessions upon logout or termination.
- 2852 3. Test results showing the product rejects invalidated session identifiers on subsequent use.
- 2853 4. Test results showing the product invalidates sessions upon authentication credential change.
- 2854 5. Test results showing the product invalidates sessions upon timeout expiration.
- 2855 6. Test results showing the product invalidates sessions without observable delay for all triggers.

2856

2857 [\[AC-AUTH-3-04\]](#) Verify that the product protects session identifiers by (i) transmitting them only over secure channels
2858 using state of the art cryptography; (ii) implementing session token protection mechanisms; and (iii) preventing
2859 disclosure of session identifiers in any product output.

2860 Assessment reference

2861 Requirement [\[REQ-AUTH-3-04\]](#).

2862 Assessment objective

2863 Confirm that the product protects session identifiers by transmitting them only over secure channels using state of the
2864 art cryptography, implementing session token protection mechanisms, and preventing disclosure of session identifiers in
2865 any product output.

2866 Assessment preparation

- 2867 1. The product is in specific operational state with at least one authenticated session.
- 2868 2. Documentation describing the secure channel, session token protection mechanisms, and the product outputs
2869 subject to session identifier disclosure controls is available.

2870 Assessment activities

- 2871 1. Review documentation to identify the secure channel protocol, the session token protection mechanism, and
2872 the product outputs subject to session identifier disclosure controls for each interface type.
- 2873 2. Capture network traffic during session establishment and use. Verify that session identifiers are transmitted
2874 only over secure channels using state of the art cryptography.
- 2875 3. Inspect the product to verify that session token protection mechanisms are active for each interface type.
- 2876 4. Inspect product outputs generated during session activity, including audit events, log entries, error messages,
2877 and diagnostics. Verify that session identifiers do not appear in any product output.
- 2878 5. Attempt to force session identifier transmission over an unencrypted channel. Verify the product does not
2879 transmit the session identifier.

2880 Assessment verdict

2881 The verdict fail is assigned if any of the following conditions apply:

- 2882 1. Documentation does not describe the secure channel protocol, the session token protection mechanism, or the
2883 product outputs subject to session identifier disclosure controls for any interface type.
- 2884 2. The product does not transmit session identifiers only over secure channels using state of the art cryptography.
- 2885 3. The product does not implement session token protection mechanisms for any interface type.
- 2886 4. The product discloses session identifiers in any product output.
- 2887 5. The product transmits session identifiers over unencrypted channels.

2888 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2889 1. Documentation describes the secure channel protocol, the session token protection mechanism, and the product
2890 outputs subject to session identifier disclosure controls for each interface type.
- 2891 2. The product transmits session identifiers only over secure channels using state of the art cryptography.
- 2892 3. The product implements session token protection mechanisms for each interface type.
- 2893 4. The product does not disclose session identifiers in any product output.
- 2894 5. The product does not transmit session identifiers over unencrypted channels.

2895 Assessment evidence

- 2896 1. Documentation describing the secure channel, session token protection mechanisms, and the product outputs
2897 subject to session identifier disclosure controls for each interface type.

- 2898 2. Test results from network traffic captures showing session identifiers are transmitted only over secure channels
2899 using state of the art cryptography.
2900 3. Test results showing session token protection mechanisms are implemented for each interface type.
2901 4. Test results showing session identifiers do not appear in any product output.
2902 5. Test results showing the product does not transmit session identifiers over unencrypted channels.
2903

2904 [\[AC-AUTH-3-05\]](#) Verify that the product limits concurrent sessions to a configurable maximum per user account.

2905 **Assessment reference**

2906 Requirement [\[REQ-AUTH-3-05\]](#).

2907 **Assessment objective**

2908 Confirm that the product limits concurrent sessions to a configurable maximum per user account.

2909 **Assessment preparation**

- 2910 1. The product is in specific operational state.
2911 2. Documentation describing the concurrent session limit mechanism is available.

2912 **Assessment activities**

- 2913 1. Review documentation to identify the default concurrent session limit and the configurable range.
2914 2. Establish sessions up to the documented limit. Verify that all are active.
2915 3. Attempt to establish one session beyond the limit. Verify that the product denies the additional session.
2916 4. Change the concurrent session limit to a different value. Verify the new limit is enforced.
2917 5. Verify the limit is enforced per user account.

2918 **Assessment verdict**

2919 The verdict fail is assigned if any of the following conditions apply:

- 2920 1. Documentation does not describe the default concurrent session limit, configurable range, and behaviour when
2921 the limit is exceeded.
2922 2. The product does not accept sessions up to the documented concurrent session limit.
2923 3. The product does not deny session establishment beyond the configured concurrent session limit.
2924 4. The product does not enforce the newly configured concurrent session limit.
2925 5. The product does not enforce the concurrent session limit independently per user account.

2926 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2927 1. Documentation describes the default concurrent session limit, configurable range, and behaviour when the
2928 limit is exceeded.
2929 2. The product accepts sessions up to the documented concurrent session limit.
2930 3. The product denies session establishment beyond the configured concurrent session limit.
2931 4. The product enforces the newly configured concurrent session limit.
2932 5. The product enforces the concurrent session limit independently per user account.

2933 **Assessment evidence**

- 2934 1. Documentation describing the concurrent session limit, configurable range, and behaviour when the limit is
2935 exceeded.
2936 2. Test results showing sessions up to the documented limit are active.
2937 3. Test results showing the product denies session establishment beyond the configured concurrent session limit.
2938 4. Test results showing the product enforces the newly configured concurrent session limit.
2939 5. Test results showing the concurrent session limit applies independently to each user account.
2940

2941 [\[AC-AUTH-3-06\]](#) Verify that the product denies privilege escalation attempts without authorization within active
2942 sessions.

2943 **Assessment reference**

2944 Requirement [\[REQ-AUTH-3-06\]](#).

2945 **Assessment objective**

2946 Confirm that the product denies privilege escalation attempts without authorization within active sessions.

2947 **Assessment preparation**

- 2948 1. The product is in specific operational state with at least one non-management authenticated session.
- 2949 2. Documentation describing the privilege escalation denial mechanism is available.

2950 **Assessment activities**

- 2951 1. Review documentation to identify the privilege escalation denial mechanism.
- 2952 2. Attempt privilege escalation from a non-management session through (i) parameter manipulation; and (ii)
- 2953 session attribute tampering. Verify the product denies each attempt.

2954 **Assessment verdict**

2955 The verdict fail is assigned if any of the following conditions apply:

- 2956 1. Documentation does not describe the privilege escalation denial mechanism.
- 2957 2. The product does not deny privilege escalation attempts without authorization from non-management sessions.

2958 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2959 1. Documentation describes the privilege escalation denial mechanism.
- 2960 2. The product denies privilege escalation attempts without authorization from non-management sessions.

2961 **Assessment evidence**

- 2962 1. Documentation describing the privilege escalation denial mechanism.
- 2963 2. Test results showing the product denies privilege escalation attempts without authorization from non-
- 2964 management sessions.
- 2965

2966 **6.5.4 [AUTH-4] Protocol access control**2967 **6.5.4.1 Requirement assessments**

2968 [\[AC-AUTH-4-01\]](#) Verify that the product enables only management protocols using state of the art cryptography in
 2969 product factory default state and in product operational state.

2970 **Assessment reference**2971 Requirement [\[REQ-AUTH-4-01\]](#).2972 **Assessment objective**

2973 Confirm that the product enables only management protocols using state of the art cryptography in product factory
 2974 default state and in product operational state.

2975 **Assessment preparation**

- 2976 1. The product is in product factory default state.
- 2977 2. Documentation describing management protocols is available.

2978 **Assessment activities**

- 2979 1. Review documentation to identify all management protocols and their cryptographic protection.
- 2980 2. Inspect the product in product factory default state to enumerate all enabled management protocols. Verify
- 2981 each uses state of the art cryptography.
- 2982 3. Complete product initialization and inspect the product in product operational state to enumerate all enabled
- 2983 management protocols. Verify each uses state of the art cryptography.
- 2984 4. Capture network traffic during a management session on each enabled protocol in product operational state.
- 2985 Verify the captured traffic uses state of the art cryptography.
- 2986 5. Attempt to enable a management protocol that does not use state of the art cryptography. Verify that the
- 2987 product denies the protocol activation or informs the user.

2988 **Assessment verdict**

2989 The verdict fail is assigned if any of the following conditions apply:

- 2990 1. Documentation does not list all management protocols or their cryptographic protection.
- 2991 2. Any management protocol enabled in product factory default state does not use state of the art cryptography.
- 2992 3. Any management protocol enabled in product operational state does not use state of the art cryptography.
- 2993 4. Any enabled management protocol does not use state of the art cryptography in product operational state.
- 2994 5. The product does not deny activation of protocols terminated by the product that do not use state of the art
- 2995 cryptography.

2996 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2997 1. Documentation lists all management protocols and their cryptographic protection.
- 2998 2. All management protocols enabled in product factory default state use state of the art cryptography.
- 2999 3. All management protocols enabled in product operational state use state of the art cryptography.
- 3000 4. All enabled management protocols use state of the art cryptography in product operational state.
- 3001 5. The product denies activation of protocols terminated by the product that do not use state of the art
- 3002 cryptography.

3003 **Assessment evidence**

- 3004 1. Documentation listing all management protocols and their cryptographic protection.
- 3005 2. Test results showing all management protocols enabled in product factory default state use state of the art
- 3006 cryptography.
- 3007 3. Test results showing all management protocols enabled in product operational state use state of the art
- 3008 cryptography.
- 3009 4. Test results from network traffic captures confirming all enabled management protocols use state of the art
- 3010 cryptography in product operational state.
- 3011 5. Test results showing the product denies activation of protocols terminated by the product that do not use state
- 3012 of the art cryptography.

3013

3014 [\[AC-AUTH-4-02\]](#) Verify that the product implements rate limiting and source validation where possible, for

3015 unauthenticated protocol requests to mitigate DoS attacks against management plane and control plane interfaces.

3016 **Assessment reference**

3017 Requirement [\[REQ-AUTH-4-02\]](#).

3018 **Assessment objective**

3019 Confirm that the product implements rate limiting and source validation where possible, for unauthenticated protocol

3020 requests to mitigate DoS attacks against management plane and control plane interfaces.

3021 **Assessment preparation**

- 3022 1. The product is in specific operational state.
- 3023 2. Documentation describing the rate limiting mechanism is available.

3024 **Assessment activities**

- 3025 1. Review documentation to identify the rate limiting thresholds for each protocol that accepts requests without
- 3026 authentication.
- 3027 2. Exceed the documented rate limiting threshold on each protocol that accepts requests without authentication.
- 3028 Verify the product drops requests after the threshold is reached.
- 3029 3. Send requests without authentication below the documented rate limiting threshold on each protocol. Verify
- 3030 the product does not block them.

3031 **Assessment verdict**

3032 The verdict fail is assigned if any of the following conditions apply:

- 3033 1. Documentation does not list rate limiting thresholds for any protocol that accepts requests without
- 3034 authentication.
- 3035 2. The product does not drop requests that exceed the documented rate limiting threshold.
- 3036 3. The product blocks requests below the documented rate limiting threshold.

- 3037 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
- 3038 1. Documentation lists rate limiting thresholds for each protocol that accepts requests without authentication.
 - 3039 2. The product drops requests that exceed the documented rate limiting threshold.
 - 3040 3. The product does not block requests below the documented rate limiting threshold.

3041 **Assessment evidence**

- 3042 1. Documentation listing rate limiting thresholds for each protocol that accepts requests without authentication.
- 3043 2. Test results showing the product enforces rate limiting by dropping requests exceeding the documented
- 3044 threshold.
- 3045 3. Test results showing requests below the documented rate limiting threshold are not blocked.

3046

3047 [\[AC-AUTH-4-03\]](#) Verify that the product provides capability to configure state of the art cryptography and to disable

3048 protocols that do not use state of the art cryptography.

3049 **Assessment reference**

3050 Requirement [\[REQ-AUTH-4-03\]](#).

3051 **Assessment objective**

3052 Confirm that the product provides capability to configure state of the art cryptography and to disable protocols that do

3053 not use state of the art cryptography.

3054 **Assessment preparation**

- 3055 1. The product is in specific operational state.
- 3056 2. Documentation describing cryptographic configuration and weak protocol versions is available.

3057 **Assessment activities**

- 3058 1. Review documentation to identify all protocols that do not use state of the art cryptography and the available
- 3059 configuration options.
- 3060 2. Use the configuration interface to disable a protocol that does not use state of the art cryptography, where the
- 3061 documentation states disabling is operationally feasible. Verify the product refuses a connection using the
- 3062 disabled protocol.
- 3063 3. Disable a weak protocol version using the configuration interface. Verify that the strong protocol version
- 3064 continues to function by completing a management session using it.
- 3065 4. Verify that the documentation provides a justification for each weak protocol version where disabling is not
- 3066 operationally feasible.

3067 **Assessment verdict**

3068 The verdict fail is assigned if any of the following conditions apply:

- 3069 1. Documentation does not describe all protocols that do not use state of the art cryptography and the available
- 3070 configuration options.
- 3071 2. The product does not provide configuration options to disable protocols that do not use state of the art
- 3072 cryptography where operationally feasible.
- 3073 3. The product does not refuse connections on disabled protocols.
- 3074 4. The product does not continue to support strong protocol versions after weak versions are disabled.
- 3075 5. Documentation does not list a justification for each weak protocol version where disabling is not operationally
- 3076 feasible.

3077 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3078 1. Documentation describes all protocols that do not use state of the art cryptography and the available
- 3079 configuration options.
- 3080 2. The product provides configuration options to disable protocols that do not use state of the art cryptography
- 3081 where operationally feasible.
- 3082 3. The product refuses connections on disabled protocols.
- 3083 4. The product continues to support strong protocol versions after weak versions are disabled.
- 3084 5. Documentation lists a justification for each weak protocol version where disabling is not operationally feasible.

3085 Assessment evidence

- 3086 1. Documentation describing all protocols that do not use state of the art cryptography and the available
3087 configuration options.
- 3088 2. Test results showing the product provides configuration options to disable protocols that do not use state of the
3089 art cryptography where operationally feasible.
- 3090 3. Test results showing the product refuses connections on disabled protocols.
- 3091 4. Test results showing the strong protocol version continues to function after weak versions are disabled.
- 3092 5. Documentation listing a justification for each weak protocol version where disabling is not operationally
3093 feasible.

3094

3095 [\[AC-AUTH-4-04\]](#) Verify that the product validates trust establishment using additional mechanisms and generates audit
3096 events for all trust relationship changes.

3097 Assessment reference

3098 Requirement [\[REQ-AUTH-4-04\]](#).

3099 Assessment objective

3100 Confirm that the product validates trust establishment using additional mechanisms and that the product generates audit
3101 events for all trust relationship changes.

3102 Assessment preparation

- 3103 1. The product is in specific operational state.
- 3104 2. Documentation describing trust establishment protocols and validation mechanisms is available.

3105 Assessment activities

- 3106 1. Review documentation to identify protocols that establish trust without cryptographic verification and the
3107 additional validation mechanisms for each.
- 3108 2. Trigger a trust establishment event for each identified protocol. Verify the additional validation mechanism
3109 operates.
- 3110 3. Attempt to establish a trust relationship through a spoofed source or a source without authorization. Verify the
3111 validation mechanism detects or mitigates the attempt.
- 3112 4. Verify that the product generates audit events for all trust relationship changes.

3113 Assessment verdict

3114 The verdict fail is assigned if any of the following conditions apply:

- 3115 1. Documentation does not list trust establishment protocols or their additional validation mechanisms.
- 3116 2. The product does not operate additional validation mechanisms during trust establishment events.
- 3117 3. The product does not detect or mitigate spoofed trust establishment attempts via validation mechanisms.
- 3118 4. The product does not generate audit events for all trust relationship changes.

3119 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3120 1. Documentation lists trust establishment protocols and their additional validation mechanisms.
- 3121 2. The product operates additional validation mechanisms during trust establishment events.
- 3122 3. The product detects or mitigates spoofed trust establishment attempts via validation mechanisms.
- 3123 4. The product generates audit events for all trust relationship changes.

3124 Assessment evidence

- 3125 1. Documentation listing trust establishment protocols and their additional validation mechanisms.
- 3126 2. Test results showing additional validation mechanisms operate during trust establishment events.
- 3127 3. Test results showing the product detects or mitigates spoofed trust establishment attempts via validation
3128 mechanisms.
- 3129 4. Test results showing audit events are generated for all trust relationship changes.

3130

3131 6.6 Data protection

3132 6.6.1 Requirement assessments

3133 [\[AC-DATA-1-01\]](#) Verify that the product protects the confidentiality of data at rest by one or more of the means in
3134 [\[RQ-DATA-1-01\]](#).

3135 **Assessment reference**

3136 Requirement [\[REQ-DATA-1-01\]](#).

3137 **Assessment objective**

3138 Confirm that, for each category of data stored by the product, the confidentiality of the data at rest is protected by (i)
3139 CRY-SOTA encryption, (ii) access controls preventing read access by unauthorized entities, or (iii) another technical
3140 means demonstrated to provide equivalent protection against unauthorized disclosure.

3141 **Assessment preparation**

- 3142 1. The product is in a specified operational state with at least one user account configured.
- 3143 2. Documentation is available that, for each category of data stored by the product, identifies the protection
3144 applied and which of points (i), (ii) or (iii) of [\[RQ-DATA-1-01\]](#) is relied upon.
- 3145 3. Where point (iii) is relied upon, documentation is available that identifies the technical means and
3146 demonstrates how it protects data-at-rest confidentiality against unauthorized disclosure equivalently to (i) or
3147 (ii).

3148 **Assessment activities**

- 3149 1. Review documentation to identify all categories of data stored by the product and, for each, the protection
3150 relied upon and the point of [\[RQ-DATA-1-01\]](#) invoked.
- 3151 2. For data relying on (i): verify that the cryptography is CRY-SOTA in accordance with Annex K; inspect
3152 storage to verify that the stored representation is not plaintext and is consistent with the documented
3153 protection.
- 3154 3. For data relying on (ii): verify that the documented access controls prevent read access to the stored data by
3155 unauthorized entities, and confirm by inspection or testing that the data cannot be read through the interfaces
3156 available to such entities.
- 3157 4. For data relying on (iii): verify that the documentation demonstrates how the technical means protects
3158 confidentiality against unauthorized disclosure equivalently to (i) or (ii), and verify the correctness of that
3159 demonstration. Where there is any uncertainty or ambiguity in the demonstration, request additional
3160 information before reaching a verdict. Confirm by inspection or testing that the protected data cannot be
3161 disclosed to unauthorized entities under the conditions the means is claimed to cover.

3162 **Assessment verdict**

3163 The verdict fail is assigned if any of the following conditions apply:

- 3164 1. Documentation does not identify all categories of data stored by the product, the protection relied upon for
3165 each, and the point of [\[RQ-DATA-1-01\]](#) invoked.
- 3166 2. Any category of stored data is left without any of the protections (i), (ii) or (iii).
- 3167 3. The cryptography is not CRY-SOTA, the stored representation is plaintext, or it is inconsistent with the
3168 documented protection.
- 3169 4. The access controls do not prevent read access by unauthorized entities, or testing shows that the data can be
3170 read by such an entity.
- 3171 5. The documentation does not demonstrate protection equivalent to (i) or (ii), the demonstration cannot be
3172 verified as correct, or testing shows that the data can be disclosed to an unauthorized entity; in any of these
3173 cases the data at rest is assessed as if stored in plaintext.

3174 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3175 1. Documentation identifies all categories of data stored by the product, the protection relied upon for each, and
3176 the point of [\[RQ-DATA-1-01\]](#) invoked.
- 3177 2. Every category of stored data is covered by at least one of (i), (ii) or (iii).
- 3178 3. The cryptography is CRY-SOTA, the stored representation is not plaintext, and the stored representation is
3179 consistent with the documented protection.

- 3180 4. The access controls prevent read access by unauthorized entities, and testing shows that the data cannot be read
 3181 by such an entity.
 3182 5. The documentation demonstrates protection equivalent to (i) or (ii), the demonstration is verified as correct,
 3183 and testing shows that the data cannot be disclosed to an unauthorized entity.

3184 **Assessment evidence**

- 3185 1. Documentation listing all categories of data stored by the product, the protection relied upon for each, and the
 3186 point of [RQ-DATA-1-01] invoked.
 3187 2. Test results showing CRY-SOTA cryptography and the absence of plaintext storage.
 3188 3. Documentation and test results showing that access controls prevent read access by unauthorized entities.
 3189 4. The technical documentation demonstrating equivalent protection, and test results showing that the protected
 3190 data cannot be disclosed to unauthorized entities.
 3191

3192 [\[AC-DATA-1-02\]](#) Verify that the product protects management communications and control plane traffic using state of
 3193 the art cryptography.

3194 **Assessment reference**

3195 Requirement [\[REQ-DATA-1-02\]](#).

3196 **Assessment objective**

3197 Confirm that the product protects management communications and control plane traffic using state of the art
 3198 cryptography.

3199 **Assessment preparation**

- 3200 1. The product is in specific operational state with management and control plane traffic actively flowing.
 3201 2. Documentation describing management communication channels and control plane protocols is available.

3202 **Assessment activities**

- 3203 1. Review documentation to identify all management communication channels and control plane protocols.
 3204 Verify the documented cryptography is state of the art.
 3205 2. Inspect network traffic during active management and control plane exchanges. Verify the captured traffic uses
 3206 state of the art cryptography.
 3207 3. Attempt to disable the cryptographic protection of management communications and control plane traffic.
 3208 Verify the product does not permit this silently or without documented justification.

3209 **Assessment verdict**

3210 The verdict fail is assigned if any of the following conditions apply:

- 3211 1. Documentation does not list all management channels or control plane protocols.
 3212 2. The product does not use state of the art cryptography for any management channel or control plane protocol.
 3213 3. The product does not use state of the art cryptography for management communications or control plane
 3214 traffic.
 3215 4. The product permits cryptographic protection of management communications to be disabled.
 3216 5. The product permits cryptographic protection of control plane traffic to be disabled.

3217 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3218 1. Documentation lists all management channels and control plane protocols.
 3219 2. The product uses state of the art cryptography for all management channels and control plane protocols.
 3220 3. The product uses state of the art cryptography for management communications and control plane traffic.
 3221 4. The product does not permit cryptographic protection of management communications to be disabled.
 3222 5. The product does not permit cryptographic protection of control plane traffic to be disabled.

3223 **Assessment evidence**

- 3224 1. Documentation listing all management channels and control plane protocols.
 3225 2. Test results showing state of the art cryptography for all management channels and control plane protocols.
 3226 3. Test results from network traffic captures during management and control plane exchanges showing state of
 3227 the art cryptography.

- 3228 4. Test results showing the product does not permit cryptographic protection of management communications to
3229 be disabled.
- 3230 5. Test results showing the product does not permit cryptographic protection of control plane traffic to be
3231 disabled.
- 3232

3233 [\[AC-DATA-1-03\]](#) Verify that the product prevents modification of configuration and firmware without authorization.

3234 **Assessment reference**

3235 Requirement [\[REQ-DATA-1-03\]](#).

3236 **Assessment objective**

3237 Confirm that the product prevents modification of configuration and firmware without authorization.

3238 **Assessment preparation**

- 3239 1. The product is in specific operational state.
- 3240 2. Documentation describing the integrity verification mechanisms for configuration files and firmware images is
3241 available.

3242 **Assessment activities**

- 3243 1. Review documentation to identify the integrity verification mechanisms and the authorization level required
3244 for modification of each.
- 3245 2. Attempt to modify a configuration file using an authorized account. Verify that the modification succeeds.
- 3246 3. Attempt to modify a configuration file using an insufficiently privileged account. Verify the modification is
3247 denied.
- 3248 4. Modify a configuration file directly on the storage medium where direct storage access is feasible. Verify the
3249 product detects, rejects, or reverts the modification.
- 3250 5. Attempt to install a tampered firmware image. Verify that the product detects the modification and rejects
3251 installation.
- 3252 6. Install the valid firmware image using an authorized account. Verify installation succeeds.

3253 **Assessment verdict**

3254 The verdict fail is assigned if any of the following conditions apply:

- 3255 1. Documentation does not describe integrity verification mechanisms for configuration files or firmware images.
- 3256 2. Documentation does not describe the authorization level required for modification of each.
- 3257 3. The product does not accept configuration modifications by authorized accounts.
- 3258 4. The product does not deny configuration modifications by insufficiently privileged accounts.
- 3259 5. The product does not detect or prevent direct storage modification of configuration files.
- 3260 6. The product does not detect and reject tampered firmware images.
- 3261 7. The product does not install valid firmware successfully with an authorized account.

3262 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3263 1. Documentation describes integrity verification mechanisms for configuration files and firmware images.
- 3264 2. Documentation describes the authorization level required for modification of each.
- 3265 3. The product accepts configuration modifications by authorized accounts.
- 3266 4. The product denies configuration modifications by insufficiently privileged accounts.
- 3267 5. The product detects or prevents direct storage modification of configuration files.
- 3268 6. The product detects and rejects tampered firmware images.
- 3269 7. The product installs valid firmware successfully with an authorized account.

3270 **Assessment evidence**

- 3271 1. Documentation describing the integrity verification mechanisms for configuration files and firmware images.
- 3272 2. Documentation describing the authorization level required for modification of each.
- 3273 3. Test results showing the product accepts configuration modifications by authorized accounts.
- 3274 4. Test results showing the product denies configuration modifications by insufficiently privileged accounts.

- 3275 5. Test results showing that direct storage modification of configuration files is detected or rejected where
 3276 feasible.
 3277 6. Test results showing that the product detects and rejects a tampered firmware image.
 3278 7. Test results showing that valid firmware installation succeeds with an authorized account.
 3279

3280 [\[AC-DATA-1-04\]](#) Verify that the product implements data protection measures ensuring the product processes and
 3281 retains only the minimum data necessary for its intended (i) routing; (ii) switching; (iii) modem functions; or (iv) any
 3282 additional product capabilities, including those described in clause [4.2.6](#).

3283 **Assessment reference**

3284 Requirement [\[REQ-DATA-1-04\]](#).

3285 **Assessment objective**

3286 Confirm that the product implements data protection measures ensuring the product processes and retains only the
 3287 minimum data necessary for its intended (i) routing; (ii) switching; (iii) modem functions; or (iv) any additional product
 3288 capabilities, including those described in clause [4.2.6](#).

3289 **Assessment preparation**

- 3290 1. The product is in specific operational state.
 3291 2. Documentation describing the intended product functions, additional product capabilities, and the categories of
 3292 data each function or capability processes and retains is available.

3293 **Assessment activities**

- 3294 1. Review documentation to identify the intended product functions, additional product capabilities, and the
 3295 categories of data that each function or capability processes and retains.
 3296 2. Inspect the product and review its data protection measures. Verify that the product implements data protection
 3297 measures ensuring data processing and retention are limited to the minimum necessary for the intended
 3298 functions and additional capabilities.
 3299 3. Attempt to retrieve retained data through the product. Verify data categories are consistent with documented
 3300 intended functions and additional product capabilities.
 3301 4. Capture outbound network traffic during operation. Verify the product transmits only data consistent with
 3302 documented intended functions and additional product capabilities.

3303 **Assessment verdict**

3304 The verdict fail is assigned if any of the following conditions apply:

- 3305 1. Documentation does not list the intended product functions, additional product capabilities, or the categories of
 3306 data processed and retained for each.
 3307 2. The product does not implement data protection measures that limit data processing and retention to the
 3308 minimum necessary for the intended functions and additional capabilities.
 3309 3. The product does not restrict retained data to categories consistent with documented intended functions and
 3310 additional product capabilities.
 3311 4. The product does not restrict transmitted data to categories consistent with documented intended functions and
 3312 additional product capabilities.

3313 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3314 1. Documentation lists the intended product functions, additional product capabilities, and the categories of data
 3315 processed and retained for each.
 3316 2. The product implements data protection measures that limit data processing and retention to the minimum
 3317 necessary for the intended functions and additional capabilities.
 3318 3. The product restricts retained data to categories consistent with documented intended functions and additional
 3319 product capabilities.
 3320 4. The product restricts transmitted data to categories consistent with documented intended functions and
 3321 additional product capabilities.

3322 **Assessment evidence**

- 3323 1. Documentation listing the intended product functions, additional product capabilities, and the categories of
 3324 data each function or capability processes and retains.

- 3325 2. Documentation and test results showing the product implements data protection measures limiting data
 3326 processing and retention to the minimum necessary.
 3327 3. Test results showing the product restricts retained data to categories consistent with documented intended
 3328 functions and additional product capabilities.
 3329 4. Test results from traffic capture confirming transmitted data is consistent with documented intended functions
 3330 and additional product capabilities.
 3331

3332 [\[AC-DATA-1-05\]](#) Verify that the product requires explicit opt-in configuration of any diagnostic or telemetry data
 3333 collection beyond the product's intended purpose, and that such collection is disabled by default.

3334 **Assessment reference**

3335 Requirement [\[REQ-DATA-1-05\]](#).

3336 **Assessment objective**

3337 Confirm that the product requires explicit opt-in configuration of any diagnostic or telemetry data collection beyond the
 3338 product's intended purpose, and that such collection is disabled by default.

3339 **Assessment preparation**

- 3340 1. The product is in product factory default state.
 3341 2. Documentation describing any diagnostic or telemetry data collection beyond the product's intended purpose,
 3342 the opt-in configuration mechanism, and the default state of such collection is available.

3343 **Assessment activities**

- 3344 1. Review documentation to identify any diagnostic or telemetry data collection beyond the product's intended
 3345 purpose, the opt-in configuration mechanism, and the default state of such collection.
 3346 2. Inspect the product in product factory default state. Capture outbound network traffic and verify that no
 3347 diagnostic or telemetry data beyond the product's intended purpose is collected or transmitted.
 3348 3. Attempt to enable diagnostic or telemetry data collection beyond the product's intended purpose. Verify that
 3349 enabling requires explicit opt-in configuration by an authorized user, distinct from accepting default settings.

3350 **Assessment verdict**

3351 The verdict fail is assigned if any of the following conditions apply:

- 3352 1. Documentation does not describe diagnostic and telemetry data collection beyond the product's intended
 3353 purpose, the opt-in configuration mechanism, and the default state of such collection.
 3354 2. The product collects or transmits diagnostic or telemetry data beyond the product's intended purpose in product
 3355 factory default state.
 3356 3. The product does not require explicit opt-in configuration to enable diagnostic or telemetry data collection
 3357 beyond the product's intended purpose.

3358 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3359 1. Documentation describes diagnostic and telemetry data collection beyond the product's intended purpose, the
 3360 opt-in configuration mechanism, and the default state of such collection.
 3361 2. The product does not collect or transmit any diagnostic or telemetry data beyond the product's intended
 3362 purpose in product factory default state.
 3363 3. The product requires explicit opt-in configuration to enable diagnostic or telemetry data collection beyond the
 3364 product's intended purpose.

3365 **Assessment evidence**

- 3366 1. Documentation describing diagnostic and telemetry data collection beyond the product's intended purpose, the
 3367 opt-in configuration mechanism, and the default state of such collection.
 3368 2. Test results from traffic capture confirming no diagnostic or telemetry data beyond the product's intended
 3369 purpose is collected or transmitted in product factory default state.
 3370 3. Test results showing the product requires explicit opt-in configuration to enable diagnostic or telemetry data
 3371 collection beyond the product's intended purpose.
 3372

3373 6.7 Availability and resilience

3374 6.7.1 Requirement assessments

3375 [\[AC-AVAIL-1-01\]](#) Verify that the product enforces rate limiting for each network protocol terminated by the product.

3376 Assessment reference

3377 Requirement [\[REQ-AVAIL-1-01\]](#).

3378 Assessment objective

3379 Confirm that the product enforces rate limiting for each network protocol terminated by the product.

3380 Assessment preparation

- 3381 1. The product is in specific operational state with at least one network protocol actively handling traffic.
- 3382 2. Documentation describing the rate limiting mechanisms and their configured thresholds and parameters is
- 3383 available.

3384 Assessment activities

- 3385 1. Review documentation to identify all rate limiting mechanisms, protected protocols, and their configured
- 3386 thresholds and parameters.
- 3387 2. Send legitimate traffic through the product at normal rates and record baseline throughput, response time, and
- 3388 resource utilization.
- 3389 3. Send requests to a protected protocol at a rate exceeding the documented threshold. Verify the product begins
- 3390 rejecting or delaying excess requests and that the documented threshold and time window match the observed
- 3391 enforcement point.
- 3392 4. Initiate a simulated traffic flood against the product from one source and simultaneously send legitimate traffic
- 3393 from a separate source. Verify that throughput and response time for the legitimate traffic confirm it continues
- 3394 to be processed and that essential forwarding and management functions remain operational.

3395 Assessment verdict

3396 The verdict fail is assigned if any of the following conditions apply:

- 3397 1. Documentation does not list all rate limiting mechanisms, protected protocols, thresholds, and parameters.
- 3398 2. The product does not maintain stable throughput, response time, or resource utilization under normal traffic.
- 3399 3. The product does not implement rate limiting.
- 3400 4. The product does not enforce the documented rate limiting thresholds.
- 3401 5. The product does not reject or delay excess requests beyond rate limiting thresholds.
- 3402 6. The product does not enforce a rate limiting time window that matches the documented value.
- 3403 7. The product does not continue to process legitimate traffic during simulated attack.
- 3404 8. The product does not maintain essential forwarding and management functions during attack.

3405 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3406 1. Documentation lists all rate limiting mechanisms, protected protocols, thresholds, and parameters.
- 3407 2. The product maintains stable throughput, response time, and resource utilization under normal traffic.
- 3408 3. The product implements rate limiting.
- 3409 4. The product enforces the documented rate limiting thresholds.
- 3410 5. The product rejects or delays excess requests beyond rate limiting thresholds.
- 3411 6. The product enforces a rate limiting time window that matches the documented value.
- 3412 7. The product continues to process legitimate traffic during simulated attack.
- 3413 8. The product maintains essential forwarding and management functions during attack.

3414 Assessment evidence

- 3415 1. Documentation listing all rate limiting mechanisms, protected protocols, thresholds, and parameters.
- 3416 2. Test results showing baseline throughput, response time, and resource utilization are recorded.
- 3417 3. Test results showing the product implements rate limiting.
- 3418 4. Test results showing the product enforces the documented rate limiting thresholds.
- 3419 5. Test results showing the product rejects or delays excess requests beyond rate limiting thresholds.

- 3420 6. Test results showing the observed rate limiting time window matches the documented value.
 3421 7. Test results showing legitimate traffic continues to be processed during simulated attack.
 3422 8. Test results showing forwarding and management functions remain operational during attack.
 3423

3424 [\[AC-AVAIL-1-02\]](#) Verify that the product enforces connection throttling for each connection-oriented network protocol
 3425 terminated by the product.

3426 **Assessment reference**

3427 Requirement [\[REQ-AVAIL-1-02\]](#).

3428 **Assessment objective**

3429 Confirm that the product enforces connection throttling for each connection-oriented network protocol terminated by
 3430 the product.

3431 **Assessment preparation**

- 3432 1. The product is in specific operational state with at least one connection-establishing network protocol actively
 3433 handling traffic.
 3434 2. Documentation describing the connection throttling mechanisms and their configured parameters is available.

3435 **Assessment activities**

- 3436 1. Review documentation to identify all connection throttling mechanisms, protected protocols, and their
 3437 configured parameters.
 3438 2. Initiate new connections to the product at a rate exceeding the documented connection throttling parameter.
 3439 Verify the product limits new connections.

3440 **Assessment verdict**

3441 The verdict fail is assigned if any of the following conditions apply:

- 3442 1. Documentation does not list all connection throttling mechanisms, protected protocols, and parameters.
 3443 2. The product does not implement connection throttling.
 3444 3. The product does not enforce the documented connection throttling parameters.
 3445 4. The product does not limit excess connections beyond throttling parameters.

3446 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3447 1. Documentation lists all connection throttling mechanisms, protected protocols, and parameters.
 3448 2. The product implements connection throttling.
 3449 3. The product enforces the documented connection throttling parameters.
 3450 4. The product limits excess connections beyond throttling parameters.

3451 **Assessment evidence**

- 3452 1. Documentation listing all connection throttling mechanisms, protected protocols, and parameters.
 3453 2. Test results showing the product implements connection throttling.
 3454 3. Test results showing the product enforces the documented connection throttling parameters.
 3455 4. Test results showing the product limits excess connections beyond throttling parameters.
 3456

3457 [\[AC-AVAIL-1-03\]](#) Verify that the product automatically recovers to specific operational state when DoS conditions
 3458 cease, without requiring manual intervention.

3459 **Assessment reference**

3460 Requirement [\[REQ-AVAIL-1-03\]](#).

3461 **Assessment objective**

3462 Confirm that the product automatically recovers to specific operational state when DoS conditions cease, without
 3463 requiring manual intervention, within the documented recovery time.

3464 **Assessment preparation**

- 3465 1. The product has DoS protection mechanisms activated by a simulated attack.
 3466 2. Documentation describing the automatic recovery behaviour, the specific operational state reached after
 3467 recovery, and the expected recovery time is available. The specific operational state includes but is not limited
 3468 to the operational state of the product prior to the DoS conditions.

3469 **Assessment activities**

- 3470 1. Review documentation to identify the automatic recovery behaviour, the specific operational state to which the
 3471 product recovers, and the expected recovery time.
 3472 2. Initiate a simulated traffic flood to activate the DoS protection mechanisms of the product. Verify that
 3473 protections are engaged, then cease the simulated attack entirely and record the cessation timestamp.
 3474 3. Measure the time until rate limiting, connection throttling, and legitimate traffic throughput return to normal
 3475 parameters after the simulated attack ceases.
 3476 4. Verify that recovery occurred without manual intervention.
 3477 5. Verify all essential functions are operational after recovery. Verify the product has not remained in a degraded
 3478 state.

3479 **Assessment verdict**

3480 The verdict fail is assigned if any of the following conditions apply:

- 3481 1. Documentation does not describe the automatic recovery behaviour, the specific operational state, or the
 3482 expected recovery time.
 3483 2. The product does not activate DoS protection mechanisms when a simulated traffic flood is initiated.
 3484 3. The product does not engage protections during the simulated traffic flood.
 3485 4. The product does not restore rate limiting and connection throttling to normal parameters automatically.
 3486 5. The product does not restore legitimate traffic throughput to baseline.
 3487 6. The product does not recover within the documented recovery period.
 3488 7. The product does not recover without manual intervention when DoS conditions cease.
 3489 8. Any essential function does not resume normal operation after recovery.
 3490 9. The product remains in a degraded state.

3491 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3492 1. Documentation describes the automatic recovery behaviour, the specific operational state, and the expected
 3493 recovery time.
 3494 2. The product activates DoS protection mechanisms when a simulated traffic flood is initiated.
 3495 3. The product engages protections during the simulated traffic flood.
 3496 4. The product restores rate limiting and connection throttling to normal parameters automatically.
 3497 5. The product restores legitimate traffic throughput to baseline.
 3498 6. The product recovers within the documented recovery period.
 3499 7. The product recovers without manual intervention when DoS conditions cease.
 3500 8. Each essential function resumes normal operation after recovery.
 3501 9. The product does not remain in a degraded state.

3502 **Assessment evidence**

- 3503 1. Documentation describing the automatic recovery behaviour, the specific operational state, and the expected
 3504 recovery time.
 3505 2. Test results showing the product activates DoS protection mechanisms when a simulated traffic flood is
 3506 initiated.
 3507 3. Test results showing the product engages protections during the simulated traffic flood.
 3508 4. Test results showing rate limiting and connection throttling return to normal parameters automatically after
 3509 attack cessation.
 3510 5. Test results showing legitimate traffic throughput returns to baseline after attack cessation.
 3511 6. Test results showing recovery occurs within the documented recovery period.
 3512 7. Test results showing recovery occurred without manual intervention when DoS conditions ceased.
 3513 8. Test results showing all essential functions resume normal operation after recovery.
 3514 9. Test results showing the product does not remain in a degraded state after recovery.
 3515

3516 [\[AC-AVAIL-1-04\]](#) Verify that the product generates audit events when (i) resource utilization exceeds the documented
3517 high utilization threshold; and (ii) resource utilization returns below the documented high utilization threshold.

3518 **Assessment reference**

3519 Requirement [\[REQ-AVAIL-1-04\]](#).

3520 **Assessment objective**

3521 Confirm that the product generates audit events when (i) resource utilization exceeds the documented high utilization
3522 threshold; and (ii) resource utilization returns below the documented high utilization threshold.

3523 **Assessment preparation**

- 3524 1. The product is in specific operational state.
3525 2. Documentation describing the resources monitored and their high utilization thresholds is available.

3526 **Assessment activities**

- 3527 1. Review documentation to identify the monitored resources and their high utilization thresholds.
3528 2. Record baseline utilization for each monitored resource and artificially increase utilization above the
3529 documented threshold for each resource.
3530 3. Inspect audit events. Verify that an audit event is generated for each resource that exceeds its documented high
3531 utilization threshold.
3532 4. Apply artificial load to drive each monitored resource above its documented high utilization threshold, then
3533 cease the load and allow utilization to return below the threshold. Inspect audit events for a threshold recovery
3534 audit event for each resource.
3535 5. Retrieve the audit event via the documented access interface. Verify that all utilization audit events are present
3536 and that no audit events are truncated.

3537 **Assessment verdict**

3538 The verdict fail is assigned if any of the following conditions apply:

- 3539 1. Documentation does not list monitored resources and their high utilization thresholds.
3540 2. Any monitored resource does not report baseline utilization.
3541 3. Any monitored resource does not reach utilization above the documented threshold under artificial load.
3542 4. The product does not generate an audit event when each monitored resource exceeds its documented high
3543 utilization threshold.
3544 5. The product does not generate a threshold recovery audit event when each monitored resource returns below
3545 the documented high utilization threshold.
3546 6. Any utilization audit event is not present in the audit log.
3547 7. The product does not expose audit events via the documented access interface.

3548 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3549 1. Documentation lists monitored resources and their high utilization thresholds.
3550 2. Each monitored resource reports baseline utilization.
3551 3. Each monitored resource reaches utilization above the documented threshold under artificial load.
3552 4. The product generates an audit event when each monitored resource exceeds its documented high utilization
3553 threshold.
3554 5. The product generates a threshold recovery audit event when each monitored resource returns below the
3555 documented high utilization threshold.
3556 6. Each utilization audit event is present in the audit log.
3557 7. The product exposes audit events via the documented access interface.

3558 **Assessment evidence**

- 3559 1. Documentation listing monitored resources and their high utilization thresholds.
3560 2. Test results showing each monitored resource reports baseline utilization.
3561 3. Test results showing each monitored resource reaches utilization above the documented threshold under
3562 artificial load.
3563 4. Test results showing an audit event is generated for each resource that exceeds its high utilization threshold.

- 3564 5. Test results showing a threshold recovery audit event is generated for each resource after utilization returns
 3565 below the documented high utilization threshold.
 3566 6. Test results showing each utilization audit event is present in the audit log.
 3567 7. Test results showing the product exposes audit events via the documented access interface.
 3568

3569 6.8 Attack surface and mitigation

3570 6.8.1 [INTEGRITY-1] System integrity and boot process

3571 6.8.1.1 Requirement assessments

3572 [\[AC-INTEGRITY-1-01\]](#) Verify that the product verifies boot component integrity using state of the art cryptography.

3573 **Assessment reference**

3574 Requirement [\[REQ-INTEGRITY-1-01\]](#).

3575 **Assessment objective**

3576 Confirm that the product verifies boot component integrity using state of the art cryptography.

3577 **Assessment preparation**

- 3578 1. The product is in product factory default state with the boot process ready to be initiated.
 3579 2. Documentation describing boot components subject to cryptographic verification is available.

3580 **Assessment activities**

- 3581 1. Review documentation to identify the boot verification scheme and failure behaviour. Verify the documented
 3582 cryptography is state of the art.
 3583 2. Boot the product and observe boot diagnostic output. Verify the product reports successful verification of each
 3584 documented boot component.
 3585 3. Modify one software boot component that is accessible for modification and attempt to boot the product.
 3586 Verify the product detects the modification, refuses to execute the modified component, and enters the
 3587 predefined failure state.
 3588 4. Modify a software boot component that is accessible for modification, then restore the original. Verify the
 3589 product completes normally after the original component is restored.
 3590 5. Inspect the verification key storage. Verify the key is stored in the documented protected location and is not
 3591 modifiable through normal product interfaces.

3592 **Assessment verdict**

3593 The verdict fail is assigned if any of the following conditions apply:

- 3594 1. Documentation does not list all boot components, verification scheme, and failure behaviour.
 3595 2. The product does not use state of the art cryptography for boot component verification.
 3596 3. Any boot component is not cryptographically verified before execution.
 3597 4. The product does not detect or does not refuse to execute a modified boot component.
 3598 5. The product does not enter the predefined failure state on verification failure.
 3599 6. The product does not complete the boot process after restoring the original boot component during
 3600 cryptographic verification testing.
 3601 7. The product does not store the verification key in the documented protected location.
 3602 8. The product permits modification of the verification key through normal product interfaces.

3603 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3604 1. Documentation lists all boot components, verification scheme, and failure behaviour.
 3605 2. The product uses state of the art cryptography for boot component verification.
 3606 3. All boot components are cryptographically verified before execution.
 3607 4. The product detects and refuses to execute a modified boot component.
 3608 5. The product enters the predefined failure state on verification failure.

- 3609 6. The product completes the boot process after restoring the original boot component during cryptographic
 3610 verification testing.
 3611 7. The product stores the verification key in the documented protected location.
 3612 8. The product does not permit modification of the verification key through normal product interfaces.

3613 **Assessment evidence**

- 3614 1. Documentation listing all boot components, verification scheme, and failure behaviour.
 3615 2. Test results showing the boot verification uses state of the art cryptography.
 3616 3. Test results showing all boot components are cryptographically verified before execution.
 3617 4. Test results showing the product detects and refuses to execute a modified boot component.
 3618 5. Test results showing the product enters the predefined failure state on verification failure.
 3619 6. Test results showing the product completes the boot process after restoring the original boot component during
 3620 cryptographic verification testing.
 3621 7. Test results showing the verification key is stored in the documented protected location.
 3622 8. Test results showing the verification key is not modifiable through normal product interfaces.
 3623

3624 [\[AC-INTEGRITY-1-02\]](#) Verify that the product in the factory default state enforces a secure boot chain where (i) each
 3625 stage of the boot chain verifies the next stage before transferring execution control; (ii) the trusted code which is the
 3626 first stage of the secure boot chain is protected against unauthorized modification; (iii) the product enters a predefined
 3627 failure state on verification failure; and (iv) only verified code executes during boot.

3628 **Assessment reference**

3629 Requirement [\[REQ-INTEGRITY-1-02\]](#).

3630 **Assessment objective**

3631 Confirm that the product in the factory default state enforces a secure boot chain where (i) each stage of the boot chain
 3632 verifies the next stage before transferring execution control; (ii) the trusted code which is the first stage of the secure
 3633 boot chain is protected against unauthorized modification; (iii) the product enters a predefined failure state on
 3634 verification failure; and (iv) only verified code executes during boot.

3635 **Assessment preparation**

- 3636 1. The product is in product factory default state with the boot process ready to be initiated.
 3637 2. Documentation describing the boot chain architecture is available.

3638 **Assessment activities**

- 3639 1. Review documentation to identify all boot stages and the verification mechanism for each stage transition.
 3640 2. Attempt to modify the trusted code which is the first stage of the secure boot chain through software means.
 3641 Verify the product rejects the modification.
 3642 3. Inspect the storage medium of the trusted code which is the first stage of the secure boot chain where
 3643 physically feasible. Verify the protection matches the documented mechanism.
 3644 4. Boot the product and observe boot diagnostic output. Verify each documented stage transition includes a
 3645 verification step before control transfer.
 3646 5. Modify a component at an intermediate boot stage and attempt to boot the product. Verify the product enters
 3647 the predefined failure state without executing the modified component.
 3648 6. Restore all components. Verify the product completes the boot process.

3649 **Assessment verdict**

3650 The verdict fail is assigned if any of the following conditions apply:

- 3651 1. Documentation does not describe all boot stages, verification mechanisms, and protection of the trusted code
 3652 which is the first stage of the secure boot chain.
 3653 2. The product does not prevent modification of the trusted code which is the first stage of the secure boot chain
 3654 through software.
 3655 3. The product does not store the trusted code which is the first stage of the secure boot chain using the
 3656 documented protection mechanism.
 3657 4. Any boot stage does not verify the next stage before transferring control.
 3658 5. The product does not enter the predefined failure state on verification failure.

- 3659 6. The product executes modified components.
 3660 7. The product does not complete the boot process after restoring all modified components.

3661 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3662 1. Documentation describes all boot stages, verification mechanisms, and protection of the trusted code which is
 3663 the first stage of the secure boot chain.
 3664 2. The product prevents modification of the trusted code which is the first stage of the secure boot chain through
 3665 software.
 3666 3. The product stores the trusted code which is the first stage of the secure boot chain using the documented
 3667 protection mechanism.
 3668 4. Each boot stage verifies the next stage before transferring control.
 3669 5. The product enters the predefined failure state on verification failure.
 3670 6. The product does not execute modified components.
 3671 7. The product completes the boot process after restoring all modified components.

3672 **Assessment evidence**

- 3673 1. Documentation describing all boot stages, verification mechanisms, and protection of the trusted code which is
 3674 the first stage of the secure boot chain.
 3675 2. Test results from modification attempt show the product rejects modification of the trusted code which is the
 3676 first stage of the secure boot chain through software.
 3677 3. Test results from storage inspection of the trusted code which is the first stage of the secure boot chain show
 3678 the storage matches the documented protection mechanism.
 3679 4. Test results showing each boot stage verifies the next stage before transferring control.
 3680 5. Test results showing the product enters the predefined failure state on verification failure.
 3681 6. Test results showing the product does not execute modified components.
 3682 7. Test results showing the product completes the boot process after restoring all modified components.
 3683

3684 [\[AC-INTEGRITY-1-03\]](#) Verify that the product generates audit events for all boot events including (i) boot stage
 3685 progression; (ii) verification success or failure for each component; (iii) recovery mode activation; and (iv) detected
 3686 bypass attempts.

3687 **Assessment reference**

3688 Requirement [\[REQ-INTEGRITY-1-03\]](#).

3689 **Assessment objective**

3690 Confirm that the product generates audit events for all boot events including (i) boot stage progression; (ii) verification
 3691 success or failure for each component; (iii) recovery mode activation; and (iv) detected bypass attempts.

3692 **Assessment preparation**

- 3693 1. The product is in product factory default state with the boot process ready to be initiated.
 3694 2. Documentation describing audit events generated during the boot process is available.

3695 **Assessment activities**

- 3696 1. Review documentation to identify all boot-related audit events and their expected content.
 3697 2. Boot the product and inspect audit events after boot completion. Verify an audit event is generated for each
 3698 boot stage progression and for each verified boot component.
 3699 3. Modify a software boot component that is accessible for modification to trigger a verification failure and boot
 3700 the product. Verify an audit event is generated for the verification failure and that audit events are accessible
 3701 after halt or recovery.
 3702 4. Trigger recovery mode entry where the product supports recovery mode and inspect audit events. Verify an
 3703 audit event is generated for recovery mode activation.
 3704 5. Attempt a boot bypass where feasible and inspect audit events. Verify an audit event is generated for the
 3705 bypass attempt.

3706 **Assessment verdict**

3707 The verdict fail is assigned if any of the following conditions apply:

- 3708 1. Documentation does not describe all boot-related audit events and their expected content.
 3709 2. The product does not generate an audit event for any boot stage progression.
 3710 3. The product does not generate an audit event for verification success for any boot component.
 3711 4. The product does not generate an audit event for boot component verification failure.
 3712 5. The product does not make audit events accessible after a verification failure boot attempt.
 3713 6. The product does not generate an audit event for recovery mode activation where recovery mode is present.
 3714 7. The product does not generate an audit event for bypass attempts where bypass detection is supported.

3715 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3716 1. Documentation describes all boot-related audit events and their expected content.
 3717 2. The product generates an audit event for each boot stage progression.
 3718 3. The product generates an audit event for verification success for each boot component.
 3719 4. The product generates an audit event for boot component verification failure.
 3720 5. The product makes audit events accessible after a verification failure boot attempt.
 3721 6. The product generates an audit event for recovery mode activation where recovery mode is present.
 3722 7. The product generates an audit event for bypass attempts where bypass detection is supported.

3723 **Assessment evidence**

- 3724 1. Documentation describing all boot-related audit events and their expected content.
 3725 2. Test results showing an audit event is generated for each boot stage progression.
 3726 3. Test results showing an audit event is generated for verification success for each boot component.
 3727 4. Test results showing the product generates an audit event for boot component verification failure.
 3728 5. Test results showing the product makes audit events accessible after a verification failure boot attempt.
 3729 6. Test results showing the product generates an audit event for recovery mode activation where recovery mode is present.
 3730 7. Test results showing the product generates an audit event for bypass attempts where bypass detection is supported.

3734 [\[AC-INTEGRITY-1-04\]](#) Verify that the product requires authentication and authorization before granting access to
 3735 recovery and maintenance modes, where such modes are present.

3736 **Assessment reference**

3737 Requirement [\[REQ-INTEGRITY-1-04\]](#).

3738 **Assessment objective**

3739 Confirm that the product shall protect recovery and maintenance modes, by using methods documented in the
 3740 instructions to the user.

3741 **Assessment preparation**

- 3742 1. The product is in product operational state.
 3743 2. Documentation describing recovery and maintenance modes is available.

3744 **Assessment activities**

- 3745 1. Review documentation to determine whether recovery mode and maintenance mode are present and to identify
 3746 the methods to protect each present mode.
 3747 2. Attempt to enter each present mode without following documented methods. Verify access is denied.
 3748 3. Attempt to enter each present mode following documented methods. Verify access is granted.
 3749 4. Inspect the product for undocumented recovery or maintenance entry points where documentation states no
 3750 such modes are present. Verify that none exist.

3751 **Assessment verdict**

3752 The verdict fail is assigned if any of the following conditions apply:

- 3753 1. Documentation does not describe recovery or maintenance mode presence.
 3754 2. The product does not protect recovery and maintenance modes by using methods documented in the
 3755 instructions to the user.

- 3756 3. Any present mode is accessible without following documented methods.
 3757 4. The product does not grant access to any present mode following documented methods.
 3758 5. An undocumented recovery or maintenance entry point exists where documentation states no such modes are
 3759 present.

3760 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3761 1. Documentation identifies recovery and maintenance mode presence, entry methods, and requirements.
 3762 2. The product protects recovery and maintenance modes by using methods documented in the instructions to the
 3763 user.
 3764 3. The product denies access to each present mode when not following documented methods.
 3765 4. The product grants access to each present mode following documented methods.
 3766 5. No undocumented recovery or maintenance entry points exist where documentation states no such modes are
 3767 present.

3768 **Assessment evidence**

- 3769 1. Documentation describing recovery and maintenance mode presence and the documented protection
 3770 mechanisms in the instructions to the user.
 3771 2. Test results from not following documented methods showing access is denied for each present mode.
 3772 3. Test results confirming access is granted following documented methods.
 3773 4. Test results from the undocumented entry point probe confirming no undocumented recovery or maintenance
 3774 entry points exist where no modes are declared.
 3775

3776 6.8.2 [PACKET-1] Default packet disposition

3777 6.8.2.1 Requirement assessments

3778 [\[AC-PACKET-1-01\]](#) Verify that the product drops any packet for which it cannot determine any processing action that
 3779 is based on implemented protocol handlers, forwarding rules, or state machines, including (i) packets with unrecognized
 3780 protocol identifiers or type fields; (ii) packets with invalid or unexpected encapsulation combinations; (iii) packets that
 3781 require processing beyond the implemented protocol stack depth of the product; (iv) packets whose header field values
 3782 fall outside the ranges specified by applicable protocol standards; (v) packets that do not match existing connection state
 3783 for stateful protocols; and (vi) any packet that triggers undefined behaviour in the product.

3784 **Assessment reference**

3785 Requirement [\[REQ-PACKET-1-01\]](#).

3786 **Assessment objective**

3787 Confirm that the product drops any packet for which it cannot determine any processing action that is based on
 3788 implemented protocol handlers, forwarding rules, or state machines, including (i) packets with unrecognized protocol
 3789 identifiers or type fields; (ii) packets with invalid or unexpected encapsulation combinations; (iii) packets that require
 3790 processing beyond the implemented protocol stack depth of the product; (iv) packets whose header field values fall
 3791 outside the ranges specified by applicable protocol standards; (v) packets that do not match existing connection state for
 3792 stateful protocols; and (vi) any packet that triggers undefined behaviour in the product.

3793 **Assessment preparation**

- 3794 1. The product is in specific operational state with at least one forwarding interface active.
 3795 2. Documentation describing packet processing behaviour is available.
 3796 3. Network traffic capture tools are available on the egress side of the product to verify packets are not
 3797 forwarded.

3798 **Assessment activities**

- 3799 1. Review documentation to identify the documented packet dropping behaviour and confirm that the product
 3800 drops the entire packet when validation fails at any protocol layer.
 3801 2. Inject packets with unrecognized protocol identifiers or type fields. Verify via egress capture that the product
 3802 drops these packets.
 3803 3. Inject packets with invalid or unexpected encapsulation combinations. Verify via egress capture that the
 3804 product drops these packets.

- 3805 4. Inject packets that require processing beyond the implemented protocol stack depth. Verify via egress capture
3806 that the product drops these packets.
- 3807 5. Inject packets with header field values outside the ranges specified in applicable protocol standards. Verify via
3808 egress capture that the product drops these packets.
- 3809 6. Inject packets that do not match existing connection state for stateful protocols. Verify via egress capture that
3810 the product drops these packets.
- 3811 7. Inject packets designed to trigger undefined behaviour in the product. Verify via egress capture that the
3812 product drops these packets.
- 3813 8. Craft packets with validation failures at (i) L2; (ii) L3; and (iii) L4 separately. Verify that the entire packet is
3814 dropped at each layer.

3815 **Assessment verdict**

3816 The verdict fail is assigned if any of the following conditions apply:

- 3817 1. Documentation does not describe packet dropping behaviour for unrecognized, invalid, and malformed
3818 packets.
- 3819 2. Documentation does not describe the entire packet dropping when validation fails at any protocol layer.
- 3820 3. The product does not drop packets with unrecognized protocol identifiers or type fields.
- 3821 4. The product does not drop packets with invalid or unexpected encapsulation combinations.
- 3822 5. The product does not drop packets that exceed the implemented protocol stack depth.
- 3823 6. The product does not drop packets with header field values outside protocol standard ranges.
- 3824 7. The product does not drop packets unmatched to connection state for stateful protocols.
- 3825 8. The product does not drop packets that trigger undefined behaviour.
- 3826 9. The product does not drop packets failing validation at any single protocol layer entirely.

3827 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3828 1. Documentation describes packet dropping behaviour for unrecognized, invalid, and malformed packets.
- 3829 2. Documentation describes the entire packet dropping when validation fails at any protocol layer.
- 3830 3. The product drops packets with unrecognized protocol identifiers or type fields.
- 3831 4. The product drops packets with invalid or unexpected encapsulation combinations.
- 3832 5. The product drops packets that exceed the implemented protocol stack depth.
- 3833 6. The product drops packets with header field values outside protocol standard ranges.
- 3834 7. The product drops packets unmatched to connection state for stateful protocols.
- 3835 8. The product drops packets that trigger undefined behaviour.
- 3836 9. The product drops packets failing validation at any single protocol layer entirely.

3837 **Assessment evidence**

- 3838 1. Documentation describing packet dropping behaviour for unrecognized, invalid, and malformed packets.
- 3839 2. Documentation describing the entire packet dropping when validation fails at any protocol layer.
- 3840 3. Test results from egress capture confirming the product drops packets with unrecognized protocol identifiers or
3841 type fields.
- 3842 4. Test results from egress capture confirming the product drops packets with invalid or unexpected
3843 encapsulation combinations.
- 3844 5. Test results from egress capture confirming the product drops packets that exceed the implemented protocol
3845 stack depth.
- 3846 6. Test results from egress capture confirming the product drops packets with header field values outside protocol
3847 standard ranges.
- 3848 7. Test results from egress capture confirming the product drops packets unmatched to connection state for
3849 stateful protocols.
- 3850 8. Test results from egress capture confirming the product drops packets that trigger undefined behaviour.
- 3851 9. Test results for L2 validation failure show the entire packet is dropped and no upper-layer processing occurs.
- 3852 10. Test results for L3 validation failure show the entire packet is dropped.
- 3853 11. Test results for L4 validation failure show the entire packet is dropped and no forwarding by lower layers
3854 occurs.
- 3855

3856 6.8.3 [EXPOSURE-1] Interface and service exposure minimization

3857 6.8.3.1 Requirement assessments

3858 [\[AC-EXPOSURE-1-01\]](#) Verify that the product enables only those interfaces and services that have been configured,
3859 regardless of the product state.

3860 **Assessment reference**

3861 Requirement [\[REQ-EXPOSURE-1-01\]](#).

3862 **Assessment objective**

3863 Confirm that the product enables only configured interfaces and services in each applicable product state, and that no
3864 additional interfaces or services are active.

3865 **Assessment preparation**

- 3866 1. The product can be placed in each applicable product state.
- 3867 2. Documentation describing configurable interfaces and services and their configured state is available.

3868 **Assessment activities**

- 3869 1. Review documentation to identify all configurable interfaces and services and their configured state.
- 3870 2. For each applicable product state, inspect enabled interfaces and services and compare the results against the
3871 configured state. Verify no unconfigured interface or service is enabled.
- 3872 3. Change the configured state of selected interfaces and services, where supported, and verify the enabled
3873 interfaces and services follow the configured state in each applicable product state.

3874 **Assessment verdict**

3875 The verdict fail is assigned if any of the following conditions apply:

- 3876 1. Documentation does not list all configurable interfaces and services and their configured state.
- 3877 2. Any enabled interface or service is not configured to be enabled in any applicable product state.
- 3878 3. The product enables any unconfigured interface or service in any applicable product state.
- 3879 4. The product enables any selected interface or service when configured to be disabled.
- 3880 5. The product disables any selected interface or service when configured to be enabled.

3881 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3882 1. Documentation lists all configurable interfaces and services and their configured state.
- 3883 2. All enabled interfaces and services are configured to be enabled in each applicable product state.
- 3884 3. The product does not enable any unconfigured interface or service in any applicable product state.
- 3885 4. The product enables selected interfaces and services only when configured to be enabled.
- 3886 5. The product disables selected interfaces and services when configured to be disabled.

3887 **Assessment evidence**

- 3888 1. Documentation listing all configurable interfaces and services and their configured state.
- 3889 2. Test results showing all enabled interfaces and services are configured to be enabled in each applicable product
3890 state.
- 3891 3. Test results showing the product does not enable any unconfigured interface or service in any applicable
3892 product state.
- 3893 4. Test results showing selected interfaces and services follow their configured state.

3894

3895 [\[AC-EXPOSURE-1-02\]](#) Verify that the product provides capability to selectively enable or disable individual services
3896 and interfaces through configuration.

3897 **Assessment reference**

3898 Requirement [\[REQ-EXPOSURE-1-02\]](#).

3899 **Assessment objective**

3900 Confirm that the product provides capability to selectively enable or disable individual services and interfaces through
3901 configuration.

3902 **Assessment preparation**

- 3903 1. The product is in specific operational state.
3904 2. Documentation describing configuration options for enabling and disabling services and interfaces is available.

3905 **Assessment activities**

- 3906 1. Review documentation to identify which services and interfaces can be individually enabled or disabled.
3907 2. Disable and re-enable at least two configurable services. Verify the product provides the capability to disable
3908 and re-enable each through configuration.
3909 3. Disable and re-enable at least two configurable interfaces. Verify each is not operational when disabled and
3910 operational when re-enabled.
3911 4. Disable one service and one interface, then restart the product. Verify disabled configuration persists and re-
3912 enabled configuration persists after restart.

3913 **Assessment verdict**

3914 The verdict fail is assigned if any of the following conditions apply:

- 3915 1. Documentation does not list which services and interfaces are individually enabled or disabled and the
3916 configuration procedure for each.
3917 2. The product does not allow individual services to be disabled and re-enabled through configuration.
3918 3. Any disabled service is accessible or any re-enabled service is not functional.
3919 4. The product does not allow individual interfaces to be disabled and re-enabled through configuration.
3920 5. Any disabled interface remains accessible.
3921 6. Any re-enabled interface is not operational.
3922 7. The product does not maintain service or interface configuration after restart.

3923 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3924 1. Documentation lists which services and interfaces are individually enabled or disabled and the configuration
3925 procedure for each.
3926 2. The product allows individual services to be disabled and re-enabled through configuration.
3927 3. Each disabled service is inaccessible and each re-enabled service is functional.
3928 4. The product allows individual interfaces to be disabled and re-enabled through configuration.
3929 5. Each disabled interface becomes inaccessible.
3930 6. Each re-enabled interface becomes operational.
3931 7. The product maintains service and interface configuration after restart.

3932 **Assessment evidence**

- 3933 1. Documentation listing which services and interfaces are individually enabled or disabled and the configuration
3934 procedure for each.
3935 2. Test results showing the product allows individual services to be disabled and re-enabled through
3936 configuration.
3937 3. Test results showing each disabled service is inaccessible and each re-enabled service is functional.
3938 4. Test results showing the product allows individual interfaces to be disabled and re-enabled through
3939 configuration.
3940 5. Test results showing each disabled interface becomes inaccessible.
3941 6. Test results showing each re-enabled interface becomes operational.
3942 7. Test results showing the product maintains service and interface configuration after restart.
3943

3944 **6.9 Monitoring and logging**

3945 **6.9.1 Requirement assessments**

3946 [\[AC-LOG-1-01\]](#) Verify that the product generates audit events for authentication activities including (i) successful or
3947 failed authentication; (ii) account lockout triggers and releases; and (iii) authentication credential change attempts.

3948 **Assessment reference**

3949 Requirement [\[REQ-LOG-1-01\]](#).

3950 **Assessment objective**

3951 Confirm that the product generates audit events for authentication activities including (i) successful or failed
3952 authentication; (ii) account lockout triggers and releases; and (iii) authentication credential change attempts.

3953 **Assessment preparation**

- 3954 1. The product is in specific operational state with at least one user account configured and authentication failure
3955 protection enabled.
3956 2. Documentation is available describing authentication-related audit events.

3957 **Assessment activities**

- 3958 1. Review documentation to identify all authentication-related audit event types.
3959 2. Trigger each documented authentication event type in sequence including (i) successful authentication; (ii)
3960 failed authentication; (iii) account lockout trigger; (iv) account lockout release; (v) successful authentication
3961 credential change; and (vi) failed authentication credential change. Verify an audit event is generated for each.
3962 3. Verify that all authentication audit events are accessible for review.

3963 **Assessment verdict**

3964 The verdict fail is assigned if any of the following conditions apply:

- 3965 1. Documentation does not list all authentication audit event types.
3966 2. The product does not generate an audit event for each documented authentication event type including
3967 successful authentication, failed authentication, account lockout trigger, account lockout release, and
3968 authentication credential change attempt.
3969 3. Any authentication audit event is not accessible for review.

3970 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3971 1. Documentation lists all authentication audit event types.
3972 2. The product generates an audit event for each documented authentication event type including successful
3973 authentication, failed authentication, account lockout trigger, account lockout release, and authentication
3974 credential change attempt.
3975 3. All authentication audit events are accessible for review.

3976 **Assessment evidence**

- 3977 1. Documentation listing all authentication audit event types.
3978 2. Test results showing an audit event is generated for each documented authentication event type triggered in
3979 sequence including successful authentication, failed authentication, lockout trigger, lockout release, and
3980 credential change attempt.
3981 3. Test results showing all authentication audit events are present and retrievable.
3982

3983 [\[AC-LOG-1-02\]](#) Verify that the product generates audit events for all session lifecycle activities including (i) session
3984 establishment with source details; (ii) session termination with reason; (iii) failed session validation attempts; and (iv)
3985 concurrent session limit violations.

3986 **Assessment reference**

3987 Requirement [\[REQ-LOG-1-02\]](#).

3988 **Assessment objective**

3989 Confirm that the product generates audit events for all session lifecycle activities including (i) session establishment
3990 with source details; (ii) session termination with reason; (iii) failed session validation attempts; and (iv) concurrent
3991 session limit violations.

3992 **Assessment preparation**

- 3993 1. The product is in specific operational state with at least one user account and session management configured
3994 with idle timeout and concurrent session limit.

3995 2. Documentation is available describing session lifecycle audit events.

3996 **Assessment activities**

- 3997 1. Review documentation to identify all session lifecycle audit event types.
- 3998 2. Establish a session. Verify the product generates an audit event for session establishment with source details.
- 3999 3. Terminate a session by user-initiated logout, idle timeout, and management-initiated termination. Verify the product generates an audit event for each session termination with reason.
- 4000
- 4001 4. Attempt to use an invalid session identifier. Verify the product generates an audit event for the failed session validation attempt.
- 4002
- 4003 5. Exceed the concurrent session limit. Verify the product generates an audit event for the concurrent session limit violation.
- 4004
- 4005 6. Verify all session lifecycle audit events are accessible for review.

4006 **Assessment verdict**

4007 The verdict fail is assigned if any of the following conditions apply:

- 4008 1. Documentation does not list all session lifecycle audit event types.
- 4009 2. The product does not generate an audit event for session establishment with source details.
- 4010 3. The product does not generate an audit event for each session termination with reason.
- 4011 4. The product does not generate an audit event for failed session validation attempts.
- 4012 5. The product does not generate an audit event for concurrent session limit violations.
- 4013 6. Any session lifecycle audit event is not accessible for review.

4014 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 4015 1. Documentation lists all session lifecycle audit event types.
- 4016 2. The product generates an audit event for session establishment with source details.
- 4017 3. The product generates an audit event for each session termination with reason.
- 4018 4. The product generates an audit event for failed session validation attempts.
- 4019 5. The product generates an audit event for concurrent session limit violations.
- 4020 6. All session lifecycle audit events are accessible for review.

4021 **Assessment evidence**

- 4022 1. Documentation listing all session lifecycle audit event types.
- 4023 2. Test results showing the product generates an audit event for session establishment with source details.
- 4024 3. Test results showing the product generates an audit event for each session termination with reason.
- 4025 4. Test results showing the product generates an audit event for failed session validation attempts.
- 4026 5. Test results showing the product generates an audit event for concurrent session limit violations.
- 4027 6. Test results showing all session lifecycle audit events are accessible for review.
- 4028

4029 [\[AC-LOG-1-03\]](#) Verify that the product implements command authorization that generates audit events whenever execution of an unauthorized command is requested.

4030

4031 **Assessment reference**

4032 Requirement [\[REQ-LOG-1-03\]](#).

4033 **Assessment objective**

4034 Confirm that the product implements command authorization that generates audit events whenever execution of an unauthorized command is requested, and that this operates consistently across all command-capable interfaces.

4035

4036 **Assessment preparation**

- 4037 1. The product is in specific operational state with accounts at multiple privilege levels configured.
- 4038 2. Documentation is available describing audit events generated for command without authorization attempts.
- 4039 3. A list of at least three commands requiring higher privileges than the test account possesses is available.

4040 **Assessment activities**

- 4041 1. Review documentation to identify the audit events generated for command without authorization attempts.

- 4042 2. Authenticate with a lower-privilege account on the primary command interface to test audit event generation
 4043 for command without authorization by (i) attempting at least three identified higher-privilege commands; and
 4044 (ii) inspecting audit events to verify an audit event is generated for each attempt.
 4045 3. Repeat at least one command without authorization attempt on a different command-capable interface and
 4046 inspect audit events. Verify an audit event is generated and that all command authorization audit events are
 4047 accessible and not suppressed.

4048 **Assessment verdict**

4049 The verdict fail is assigned if any of the following conditions apply:

- 4050 1. Documentation does not describe the audit events generated for command without authorization attempts.
 4051 2. Any command without authorization attempt from a lower-privilege account does not generate an audit event
 4052 when attempting at least three identified higher-privilege commands.
 4053 3. The product does not generate audit events for command without authorization attempts on secondary
 4054 interfaces.
 4055 4. The product does not generate audit events consistently across all command-capable interfaces.
 4056 5. Any command authorization audit event is not accessible for review.

4057 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 4058 1. Documentation describes the audit events generated for command without authorization attempts.
 4059 2. Each command without authorization attempt from a lower-privilege account generates an audit event when
 4060 attempting at least three identified higher-privilege commands.
 4061 3. The product generates audit events for command without authorization attempts on secondary interfaces.
 4062 4. The product generates audit events consistently across all command-capable interfaces.
 4063 5. All command authorization audit events are accessible for review.

4064 **Assessment evidence**

- 4065 1. Documentation describing the audit events generated for command without authorization attempts.
 4066 2. Test results showing each command without authorization attempt from a lower-privilege account generates an
 4067 audit event when attempting higher-privilege commands.
 4068 3. Test results showing the product generates audit events for command without authorization attempts on
 4069 secondary interfaces.
 4070 4. Test results showing the product generates audit events consistently across all command-capable interfaces.
 4071 5. Test results showing all command authorization audit events are accessible for review.
 4072

4073 **6.10 Data management**

4074 **6.10.1 [TRANSFER-1] Secure data export and transfer**

4075 **6.10.1.1 Requirement assessments**

4076 [\[AC-TRANSFER-1-01\]](#) Verify that the product provides capability to transfer exported data over a channel protected
 4077 by state of the art cryptography.

4078 **Assessment reference**

4079 Requirement [\[REQ-TRANSFER-1-01\]](#).

4080 **Assessment objective**

4081 Confirm that the product provides capability to transfer exported data over a channel protected by state of the art
 4082 cryptography.

4083 **Assessment preparation**

- 4084 1. The product is in specific operational state.
 4085 2. Documentation describing the data export channel and the cryptography protecting it is available.

4086 **Assessment activities**

- 4087 1. Review documentation to identify the data export channel and the cryptography protecting it. Verify the
4088 documented cryptography is state of the art.
4089 2. Initiate a data export operation and capture network traffic during the transfer. Verify that the traffic is carried
4090 over a channel protected by state of the art cryptography and that the data export completes successfully.

4091 **Assessment verdict**

4092 The verdict fail is assigned if any of the following conditions apply:

- 4093 1. Documentation does not describe the data export channel or the cryptography protecting it.
4094 2. The product does not use state of the art cryptography on the documented channel.
4095 3. The product does not transfer exported data over a channel protected by state of the art cryptography.
4096 4. The product does not complete data export operations successfully.

4097 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 4098 1. Documentation describes the data export channel and the cryptography protecting it.
4099 2. The product uses state of the art cryptography on the documented channel.
4100 3. The product transfers exported data over a channel protected by state of the art cryptography.
4101 4. The product completes data export operations successfully.

4102 **Assessment evidence**

- 4103 1. Documentation describing the data export channel and the cryptography protecting it.
4104 2. Test results from network traffic captures showing the data export channel is protected by state of the art
4105 cryptography.
4106 3. Test results showing the data export operation completes successfully.
4107

4108 [\[AC-TRANSFER-1-02\]](#) Verify that the product provides capability to transfer imported data over a channel protected
4109 by state of the art cryptography.

4110 **Assessment reference**

4111 Requirement [\[REQ-TRANSFER-1-02\]](#).

4112 **Assessment objective**

4113 Confirm that the product provides capability to transfer imported data over a channel protected by state of the art
4114 cryptography.

4115 **Assessment preparation**

- 4116 1. The product is in specific operational state.
4117 2. Documentation describing the data import channel and the cryptography protecting it is available.

4118 **Assessment activities**

- 4119 1. Review documentation to identify the data import channel and the cryptography protecting it. Verify the
4120 documented cryptography is state of the art.
4121 2. Initiate a data import operation and capture network traffic during the transfer. Verify that the traffic is carried
4122 over a channel protected by state of the art cryptography and that the data import completes successfully.

4123 **Assessment verdict**

4124 The verdict fail is assigned if any of the following conditions apply:

- 4125 1. Documentation does not describe the data import channel or the cryptography protecting it.
4126 2. The product does not use state of the art cryptography on the documented channel.
4127 3. The product does not transfer imported data over a channel protected by state of the art cryptography.
4128 4. The product does not complete data import operations successfully.

4129 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 4130 1. Documentation describes the data import channel and the cryptography protecting it.
4131 2. The product uses state of the art cryptography on the documented channel.
4132 3. The product transfers imported data over a channel protected by state of the art cryptography.
4133 4. The product completes data import operations successfully.

4134 Assessment evidence

- 4135 1. Documentation describing the data import channel and the cryptography protecting it.
- 4136 2. Test results from network traffic captures showing the data import channel is protected by state of the art
- 4137 cryptography.
- 4138 3. Test results showing the data import operation completes successfully.
- 4139

4140 [\[AC-TRANSFER-1-03\]](#) Verify that the product requires management access for data export and data import operations.

4141 Assessment reference

4142 Requirement [\[REQ-TRANSFER-1-03\]](#).

4143 Assessment objective

4144 Confirm that the product requires management access for data export and data import operations.

4145 Assessment preparation

- 4146 1. The product is in specific operational state.
- 4147 2. Documentation describing access control requirements for data transfer operations is available.

4148 Assessment activities

- 4149 1. Review documentation to identify the access control requirements for data export and data import operations.
- 4150 2. Attempt to initiate a data export operation without management access. Verify the attempt is denied.
- 4151 3. Attempt to initiate a data import operation without management access. Verify the attempt is denied.
- 4152 4. Authenticate with a management account and perform a data export and a data import operation. Verify both
- 4153 operations complete.

4154 Assessment verdict

4155 The verdict fail is assigned if any of the following conditions apply:

- 4156 1. Documentation does not describe management access requirements for data export and data import operations.
- 4157 2. The product does not deny data export without management access.
- 4158 3. The product does not deny data import without management access.
- 4159 4. The product does not permit data export with management access.
- 4160 5. The product does not permit data import with management access.

4161 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 4162 1. Documentation describes management access requirements for data export and data import operations.
- 4163 2. The product denies data export without management access.
- 4164 3. The product denies data import without management access.
- 4165 4. The product permits data export with management access.
- 4166 5. The product permits data import with management access.

4167 Assessment evidence

- 4168 1. Documentation describing management access requirements for data export and data import operations.
- 4169 2. Test results showing the product denies data export without management access.
- 4170 3. Test results showing the product denies data import without management access.
- 4171 4. Test results showing the product permits data export with management access.
- 4172 5. Test results showing the product permits data import with management access.
- 4173

4174 [\[AC-TRANSFER-1-04\]](#) Verify that the product generates audit events for all data export and data import operations.

4175 Assessment reference

4176 Requirement [\[REQ-TRANSFER-1-04\]](#).

4177 Assessment objective

4178 Confirm that the product generates an audit event for every data export and data import operation whether successful or
4179 failed.

4180 **Assessment preparation**

- 4181 1. The product is in specific operational state.
- 4182 2. Valid data for import is available.
- 4183 3. Documentation describing the audit events generated for export and import operations is available.
- 4184 4. Management and non-management credentials are available.

4185 **Assessment activities**

- 4186 1. Review documentation to identify the audit events generated for export and import operations.
- 4187 2. Perform a data export with management credentials and inspect the audit event. Verify an audit event is
4188 generated for the operation.
- 4189 3. Attempt a data export with non-management credentials or trigger a failure. Verify an audit event is generated
4190 for the failed attempt.
- 4191 4. Perform a data import with management credentials using valid import data and inspect the audit event. Verify
4192 an audit event is generated for the operation.
- 4193 5. Attempt a data import with non-management credentials or using invalid data. Verify an audit event is
4194 generated for the failed attempt and that all events are accessible for review.

4195 **Assessment verdict**

4196 The verdict fail is assigned if any of the following conditions apply:

- 4197 1. Documentation does not describe the audit events generated for export and import operations.
- 4198 2. Any successful export operation does not generate an audit event.
- 4199 3. Any failed export attempt does not generate an audit event.
- 4200 4. Any successful import operation does not generate an audit event.
- 4201 5. Any failed import attempt does not generate an audit event.
- 4202 6. Any import audit event is not accessible for review.

4203 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 4204 1. Documentation describes the audit events generated for export and import operations.
- 4205 2. Each successful export operation generates an audit event.
- 4206 3. Each failed export attempt generates an audit event.
- 4207 4. Each successful import operation generates an audit event.
- 4208 5. Each failed import attempt generates an audit event.
- 4209 6. All import audit events are accessible for review.

4210 **Assessment evidence**

- 4211 1. Documentation describing the audit events generated for export and import operations.
- 4212 2. Test results from audit event inspection show an audit event is generated for the successful export operation.
- 4213 3. Test results from audit event inspection show an audit event is generated for the failed export attempt.
- 4214 4. Test results from audit event inspection show an audit event is generated for the successful import operation.
- 4215 5. Test results from audit event inspection show an audit event is generated for the failed import attempt.
- 4216 6. Test results showing all export and import audit events are accessible for review.

4217

4218

4219 **Annex A (informative):**
 4220 **Relationship between the present document and the**
 4221 **requirements of EU Regulation (EU) 2024/2847 - the Cyber**
 4222 **Resilience Act**

4223 The present document has been prepared under the Commission's standardisation request C(2025)618 [i.3] to provide
 4224 one voluntary means of conforming to the requirements of Regulation (EU) 2024/2847 [i.1] of the European Parliament
 4225 and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and
 4226 amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828, known as the Cyber
 4227 Resilience Act (CRA).

4228 Once the present document is cited in the Official Journal of the European Union under that Regulation, compliance
 4229 with the normative clauses of the present document given in table A.1 confers, within the limits of the scope of the
 4230 present document, a presumption of conformity with the corresponding requirements of that Regulation and associated
 4231 EFTA regulations.

4232 **Table A.1: Relationship between the present document and the requirements of Regulation (EU)**
 4233 **2024/2847 [i.1] - the Cyber Resilience Act**

Description	Essential Requirements of Regulation (EU) 2024/2847	Clause(s) of the present document	Remarks / Notes
Annex I, Part I, (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.	Clause 5.2	
Annex I, Part I, (2)(a)	Products with digital elements shall be made available on the market without known exploitable vulnerabilities.	Clause 5.3	
Annex I, Part I, (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.	Clauses 5.4.1 and 5.4.2	
Annex I, Part I, (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.	Clause 5.5.1	
Annex I, Part I, (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.	Clauses 5.6.1 , 5.6.2 , 5.6.3 and 5.6.4	
Annex I, Part I, (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.	Clause 5.7	
Annex I, Part I, (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.	Clause 5.7	
Annex I, Part I, (2)(g)	Products with digital elements shall process only data, personal or other, that are adequate, relevant and limited	Clause 5.7	

Description	Essential Requirements of Regulation (EU) 2024/2847	Clause(s) of the present document	Remarks / Notes
	to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation).		
Annex I, Part I, (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.	Clause 5.8	
Annex I, Part I, (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.	Clause 5.8	
Annex I, Part I, (2)(j)	Products with digital elements shall be designed, developed and produced to limit attack surfaces, including external interfaces.	Clauses 5.9.2 and 5.9.3	
Annex I, Part I, (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.	Clause 5.9.1	
Annex I, Part I, (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.	Clause 5.10	
Annex I, Part I, (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.	Clauses 5.4.2 and 5.11.1	

4234

4235 **Key to columns:**4236 **Description** A textual reference to the requirement.4237 **Essential Requirements of Regulation (EU) 2024/2847**4238 Identification of point(s) defining the requirement in Regulation (EU) 2024/2847 - the Cyber
4239 Resilience Act.4240 **Clause(s) of the present document**

4241 Identification of clause(s) addressing the requirement in the present document.

4242 Presumption of conformity stays valid only as long as a reference to the present document is maintained in the list
4243 published in the Official Journal of the European Union. Users of the present document should consult frequently the
4244 latest list published in the Official Journal of the European Union.

4245 Other Union legislation may be applicable to the product(s) falling within the scope of the present document.

4246

4247 **Annex B (informative):**
4248 **Security analysis**

4249 **B.1 General**

4250 This clause provides the threat and vulnerability analysis that informed the risk factor-based security requirements
4251 defined in clause 5 of the present document.

4252 First, threats are identified in relation to the product functions described in clause 4.2, the assets described in clause
4253 4.3.1, and the capabilities described in clause 4.2.6 of the present document. These threats are listed in clause B.2. In
4254 this way, the threats described in clause B.2 can be connected to the product context within which they may arise.

4255 Second, the relevance of threats is assessed based on risk factors. Given the informative nature of this annex, the
4256 assessment of threat relevance is provided in clause B.3. This framework is used to condition requirements, where
4257 applicable, on the presence of risk factors that affect the applicability and likelihood of the corresponding threats.

4258 This threat-driven approach intends to ensure that security requirements remain proportionate to actual risk while
4259 achieving the security objectives defined by the CRA.

4260 **B.2 Threat landscape**

4261 **B.2.1 Threats related to vulnerability handling**

4262

Table B.1: Threats related to vulnerability handling

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-VH-01]	Exploitation of known vulnerabilities	<ul style="list-style-type: none"> • [FN-G-01] Configuration and management • [FN-G-02] Monitoring and diagnostics • [FN-G-03] Access control • [FN-RS-01] Topology discovery • [FN-RS-02] Handling of network traffic processing rules • [FN-RS-03] Traffic access control • [FN-R-01] Routing • [FN-S-01] Switching • [FN-R-02] WAN connectivity • [FN-M-01] WAN connectivity • [FN-M-02] ISP-side remote management • [AS-DP-03] Generalized central processing units • [AS-CP-01] MAC tables • [AS-CP-02] Routing tables • [AS-CP-03] Flow tables • [AS-MP-01] Command-line interfaces • [AS-MP-02] Web-based management consoles • [AS-MP-03] Programmatic APIs • [AS-MP-04] Management software • [AS-MP-05] Management plane protocol stacks • [AS-I-01] Ethernet interfaces per the IEEE 802.3 standards family • [AS-I-02] Wi-Fi® interfaces per IEEE 802.11 • [AS-I-04] Console ports • [AS-I-05] USB interfaces • [AS-I-06] Out-of-band management interfaces • [AS-B-01] Central processing units, primarily for control and management functions • [AS-B-04] Embedded operating system • [AS-B-05] Network protocol stacks • [AS-B-06] Encryption • [CAP-01] Integrated firewall capabilities • [CAP-02] VPN services • [CAP-03] Integrated Wireless Access Point • [CAP-04] Content filtering

Threat ID	Threat title	Primarily affected functions, assets and capabilities
		<ul style="list-style-type: none"> • [CAP-05] QoS management • [CAP-06] Network monitoring tools • [CAP-07] Network segmentation • [CAP-08] Virtualization or container execution stacks • [CAP-09] PKI Certification Authority functionality • [CAP-10] Network functions related to telecommunications

4263

4264 B.2.2 Threats related to packet processing and availability of services

4265

Table B.2: Threats related to packet processing and availability of services

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-PS-01]	Interception of communication via the product	<ul style="list-style-type: none"> • [FN-RS-02] Handling of network traffic processing rules • [FN-RS-03] Traffic access control • [FN-R-01] Routing • [FN-S-01] Switching • [FN-R-02] WAN connectivity • [FN-M-01] WAN connectivity • [CAP-01] Integrated firewall capabilities • [CAP-02] VPN services • [CAP-09] PKI Certification Authority functionality • [CAP-10] Network functions related to telecommunications
[T-PS-02]	Redirection of communication to an illegitimate destination	<ul style="list-style-type: none"> • [FN-RS-01] Topology discovery • [FN-RS-02] Handling of network traffic processing rules • [FN-RS-03] Traffic access control • [FN-R-01] Routing • [FN-S-01] Switching • [FN-R-02] WAN connectivity • [FN-M-01] WAN connectivity • [AS-CP-01] MAC tables • [AS-CP-02] Routing tables • [AS-CP-03] Flow tables • [CAP-01] Integrated firewall capabilities
[T-PS-03]	Service limitation	<ul style="list-style-type: none"> • [FN-G-01] Configuration and management • [FN-G-02] Monitoring and diagnostics • [FN-RS-01] Topology discovery • [FN-RS-02] Handling of network traffic processing rules • [FN-R-01] Routing • [FN-S-01] Switching • [FN-R-02] WAN connectivity • [FN-M-01] WAN connectivity • [AS-I-01] Ethernet interfaces per the IEEE 802.3 standards family • [AS-I-02] Wi-Fi® interfaces per IEEE 802.11 • [AS-I-04] Console ports • [AS-I-05] USB interfaces • [AS-I-06] Out-of-band management interfaces • [CAP-02] VPN services • [CAP-03] Integrated Wireless Access Point • [CAP-04] Content filtering • [CAP-05] QoS management • [CAP-10] Network functions related to telecommunications
[T-PS-04]	Disruption of the availability of the product (DoS)	<ul style="list-style-type: none"> • [FN-G-01] Configuration and management • [FN-G-02] Monitoring and diagnostics • [FN-RS-01] Topology discovery • [FN-RS-02] Handling of network traffic processing rules • [FN-RS-03] Traffic access control • [FN-R-01] Routing • [FN-S-01] Switching • [FN-R-02] WAN connectivity • [FN-M-01] WAN connectivity

Threat ID	Threat title	Primarily affected functions, assets and capabilities
		<ul style="list-style-type: none"> • [FN-M-02] ISP-side remote management • [CAP-01] Integrated firewall capabilities • [CAP-02] VPN services • [CAP-03] Integrated Wireless Access Point • [CAP-04] Content filtering • [CAP-05] QoS management • [CAP-06] Network monitoring tools • [CAP-07] Network segmentation • [CAP-08] Virtualization or container execution stacks • [CAP-09] PKI Certification Authority functionality • [CAP-10] Network functions related to telecommunications
[T-PS-05]	Resource exhaustion	<ul style="list-style-type: none"> • [FN-G-01] Configuration and management • [FN-G-02] Monitoring and diagnostics • [FN-RS-01] Topology discovery • [FN-RS-02] Handling of network traffic processing rules • [FN-RS-03] Traffic access control • [FN-R-01] Routing • [FN-S-01] Switching • [FN-R-02] WAN connectivity • [FN-M-01] WAN connectivity • [FN-M-02] ISP-side remote management • [AS-DP-02] Network processors optimized for packet processing operations • [AS-DP-03] Generalized central processing units • [AS-CP-01] MAC tables • [AS-CP-02] Routing tables • [AS-CP-03] Flow tables • [AS-I-01] Ethernet interfaces per the IEEE 802.3 standards family • [AS-I-02] Wi-Fi® interfaces per IEEE 802.11 • [AS-B-01] Central processing units, primarily for control and management functions • [AS-B-02] Volatile memory • [AS-B-03] Non-volatile memory • [AS-B-06] Encryption • [CAP-01] Integrated firewall capabilities • [CAP-02] VPN services • [CAP-03] Integrated Wireless Access Point • [CAP-08] Virtualization or container execution stacks
[T-PS-06]	Deactivation of ancillary functionalities without authorization	<ul style="list-style-type: none"> • [FN-G-01] Configuration and management • [FN-G-03] Access control • [FN-M-02] ISP-side remote management • [CAP-01] Integrated firewall capabilities • [CAP-02] VPN services • [CAP-03] Integrated Wireless Access Point • [CAP-04] Content filtering • [CAP-05] QoS management • [CAP-06] Network monitoring tools • [CAP-07] Network segmentation • [CAP-08] Virtualization or container execution stacks • [CAP-09] PKI Certification Authority functionality • [CAP-10] Network functions related to telecommunications
[T-PS-07]	Activation of ancillary functions without authorization	<ul style="list-style-type: none"> • [FN-G-03] Access control • [FN-RS-03] Traffic access control • [FN-M-02] ISP-side remote management • [CAP-01] Integrated firewall capabilities • [CAP-02] VPN services • [CAP-03] Integrated Wireless Access Point • [CAP-04] Content filtering • [CAP-05] QoS management • [CAP-06] Network monitoring tools

Threat ID	Threat title	Primarily affected functions, assets and capabilities
		<ul style="list-style-type: none"> [CAP-07] Network segmentation [CAP-08] Virtualization or container execution stacks [CAP-09] PKI Certification Authority functionality [CAP-10] Network functions related to telecommunications

4266

4267 B.2.3 Threats related to access control and authentication

4268

Table B.3: Threats related to access control and authentication

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-AA-01]	Failure of access control	<ul style="list-style-type: none"> [FN-G-01] Configuration and management [FN-G-02] Monitoring and diagnostics [FN-G-03] Access control [FN-RS-02] Handling of network traffic processing rules [FN-RS-03] Traffic access control [FN-M-02] ISP-side remote management
[T-AA-02]	Bypass authentication controls	<ul style="list-style-type: none"> [FN-G-01] Configuration and management [FN-G-02] Monitoring and diagnostics [FN-G-03] Access control [FN-RS-02] Handling of network traffic processing rules [FN-RS-03] Traffic access control [FN-M-02] ISP-side remote management
[T-AA-03]	Brute force attack on user credentials	<ul style="list-style-type: none"> [FN-G-03] Access control [FN-M-02] ISP-side remote management
[T-AA-04]	Privilege escalation	<ul style="list-style-type: none"> [FN-G-01] Configuration and management [FN-G-02] Monitoring and diagnostics [FN-G-03] Access control [FN-RS-02] Handling of network traffic processing rules [FN-RS-03] Traffic access control [FN-M-02] ISP-side remote management
[T-AA-05]	Session hijacking	<ul style="list-style-type: none"> [FN-G-01] Configuration and management [FN-G-02] Monitoring and diagnostics [FN-G-03] Access control [FN-RS-02] Handling of network traffic processing rules [FN-RS-03] Traffic access control [FN-M-02] ISP-side remote management

4269

4270 B.2.4 Threats related to tampering and data processing

4271

Table B.4: Threats related to tampering and data processing

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-TD-01]	Tampering physical components of the product	<ul style="list-style-type: none"> [FN-G-01] Configuration and management [FN-RS-01] Topology discovery [FN-R-01] Routing [FN-S-01] Switching [FN-R-02] WAN connectivity [FN-M-01] WAN connectivity [AS-DP-01] Application-specific integrated circuits. [AS-DP-02] Network processors optimized for packet processing operations [AS-DP-03] Generalized central processing units [AS-I-01] Ethernet interfaces per the IEEE 802.3 standards family [AS-I-03] Fibre optic connectors [AS-I-04] Console ports [AS-I-05] USB interfaces [AS-I-06] Out-of-band management interfaces [AS-B-01] Central processing units, primarily for control and management functions

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-TD-02]	Tampering of logical components of the product	<ul style="list-style-type: none"> • [AS-B-06] Encryption • [CAP-03] Integrated Wireless Access Point • [FN-G-01] Configuration and management • [FN-G-02] Monitoring and diagnostics • [FN-G-03] Access control • [FN-RS-01] Topology discovery • [FN-RS-02] Handling of network traffic processing rules • [FN-RS-03] Traffic access control • [FN-R-01] Routing • [FN-S-01] Switching • [FN-R-02] WAN connectivity • [FN-M-01] WAN connectivity • [FN-M-02] ISP-side remote management • [AS-DP-02] Network processors optimized for packet processing operations • [AS-DP-03] Generalized central processing units • [AS-CP-01] MAC tables • [AS-CP-02] Routing tables • [AS-CP-03] Flow tables • [AS-MP-04] Management software • [AS-MP-05] Management plane protocol stacks • [AS-I-01] Ethernet interfaces per the IEEE 802.3 standards family • [AS-I-02] Wi-Fi® interfaces per IEEE 802.11 • [AS-I-04] Console ports • [AS-I-05] USB interfaces • [AS-I-06] Out-of-band management interfaces • [AS-B-04] Embedded operating system • [AS-B-05] Network protocol stacks • [AS-B-06] Encryption • [CAP-08] Virtualization or container execution stacks • [CAP-10] Network functions related to telecommunications
[T-TD-03]	Tampering of data persistently stored on the product	<ul style="list-style-type: none"> • [FN-G-01] Configuration and management • [FN-G-02] Monitoring and diagnostics • [FN-G-03] Access control • [FN-RS-02] Handling of network traffic processing rules • [FN-RS-03] Traffic access control • [FN-R-01] Routing • [FN-S-01] Switching • [FN-M-02] ISP-side remote management • [AS-CP-01] MAC tables • [AS-CP-02] Routing tables • [AS-CP-03] Flow tables • [AS-B-02] Volatile memory • [CAP-09] PKI Certification Authority functionality
[T-TD-04]	Tampering of data processed and used by the product	<ul style="list-style-type: none"> • [FN-G-01] Configuration and management • [FN-G-02] Monitoring and diagnostics • [FN-G-03] Access control • [FN-RS-01] Topology discovery • [FN-RS-02] Handling of network traffic processing rules • [FN-RS-03] Traffic access control • [FN-R-01] Routing • [FN-S-01] Switching • [FN-R-02] WAN connectivity • [FN-M-01] WAN connectivity • [FN-M-02] ISP-side remote management • [AS-CP-01] MAC tables • [AS-CP-02] Routing tables • [AS-CP-03] Flow tables • [AS-MP-05] Management plane protocol stacks • [AS-B-02] Volatile memory

Threat ID	Threat title	Primarily affected functions, assets and capabilities
		<ul style="list-style-type: none"> • [AS-B-05] Network protocol stacks • [AS-B-06] Encryption
[T-TD-05]	Installation of tampered update packages	<ul style="list-style-type: none"> • [FN-G-01] Configuration and management • [FN-G-02] Monitoring and diagnostics • [FN-G-03] Access control • [FN-RS-01] Topology discovery • [FN-RS-02] Handling of network traffic processing rules • [FN-RS-03] Traffic access control • [FN-R-01] Routing • [FN-S-01] Switching • [FN-R-02] WAN connectivity • [FN-M-01] WAN connectivity • [FN-M-02] ISP-side remote management • [AS-MP-04] Management software • [AS-MP-05] Management plane protocol stacks • [AS-B-01] Central processing units, primarily for control and management functions • [AS-B-04] Embedded operating system • [AS-B-05] Network protocol stacks • [AS-B-06] Encryption • [CAP-01] Integrated firewall capabilities • [CAP-02] VPN services • [CAP-03] Integrated Wireless Access Point • [CAP-04] Content filtering • [CAP-05] QoS management • [CAP-06] Network monitoring tools • [CAP-07] Network segmentation • [CAP-08] Virtualization or container execution stacks • [CAP-09] PKI Certification Authority functionality • [CAP-10] Network functions related to telecommunications
[T-TD-06]	Disclosure without authorization of data processed or used by the product	<ul style="list-style-type: none"> • [FN-G-01] Configuration and management • [FN-G-02] Monitoring and diagnostics • [FN-G-03] Access control • [FN-RS-02] Handling of network traffic processing rules • [FN-RS-03] Traffic access control • [FN-R-01] Routing • [FN-R-02] WAN connectivity • [FN-M-01] WAN connectivity • [FN-M-02] ISP-side remote management • [AS-CP-01] MAC tables • [AS-CP-02] Routing tables • [AS-CP-03] Flow tables • [AS-B-06] Encryption • [CAP-09] PKI Certification Authority functionality

4272

4273 B.3 Threat assessment framework

4274 B.3.1 Introduction

4275 This clause establishes an assessment framework for the threats described in clause [B.2](#). Products within scope differ
4276 widely, so not all threats apply equally to all products and deployments. Applicability depends on specific properties of
4277 the product and its operational environment.

4278 Each threat in clause [B.2](#) identifies the product functions, assets, and capabilities that contribute to the attack surface of
4279 that threat. This characterization is informative. It describes which product properties make a threat relevant but does
4280 not directly govern requirement applicability. Requirement applicability is determined by the risk factors in clause [B.3](#)
4281 and by feature-specific conditionals in clause [5](#).

4282 B.3.2 Risk factors

4283 The risk factors are organized into four categories:

- 4284 • baseline risk factors;
- 4285 • management risk factors;
- 4286 • protocol implementation risk factors;
- 4287 • data operations risk factors.

4288 Where not explicitly stated otherwise, the risk factors are deemed of equal relevance to all use cases described in clause
4289 [4.7](#).

4290 B.3.2.1 Baseline risk factors

4291 The following risk factors arise from fundamental security properties of the products within the scope of the present
4292 document:

4293

Table B.5: Baseline risk factors

ID	Title	Description
[RF-B-01]	Initial deployment risk factor	This risk factor applies to all products when first deployed as vulnerabilities identified in the timespan between the product being made available on the market and its initial deployment are still present when the product is put to service for the first time.
[RF-B-02]	Lifecycle transition risk factor	This risk factor applies when products undergo decommissioning, service returns, ownership transfers, or equipment recycling. Products retaining configuration data during lifecycle transitions can expose information such as credentials, cryptographic keys, network topology, and operational logs to parties without authorization.
[RF-B-03]	Availability disruption risk factor	This risk factor applies to all products providing network connectivity or critical services, as failure of the product cascades through dependent systems. The relevance of this risk factor increases with the number of dependent systems. It needs to be considered for devices intended for professional use, especially when these devices are deployed in provider and carrier networks or critical infrastructure.
[RF-B-04]	Boot integrity risk factor	This risk factor applies to all products executing firmware and software, as in absence of trust anchors products cannot distinguish legitimate updates from malicious modifications.
[RF-B-05]	Packet processing risk factor	This risk factor applies to all products forwarding or processing network packets in case of missing or limited packet validation as packets whose structures deviate from protocol specifications can impact the functionalities of the product by effects such as buffer overflows or memory corruption.
[RF-B-06]	Network interface exposure risk factor	This risk factor applies to all products with network interfaces, management functions, and physical ports. Every exposed interface potentially increases the attack surface of the product as it can enable additional attack vectors regardless of the position of the product within the network.

4294

4295 B.3.2.2 Management risk factors

4296 The following risk factors arise from the management of the product covering both its technical and organizational
4297 aspects:

4298

Table B.6: Management risk factors

ID	Title	Description
[RF-M-01]	Physical access exploitation risk factor	This risk factor applies when physical management interfaces lack security controls, as without corresponding measures physical access

ID	Title	Description
		directly allows modification of the behaviour of the product, for example by a change of configurations or disabling security features.
[RF-M-02]	Local network management exposure risk factor	This risk factor applies when devices support management via protocols accessible from the local network segment or broadcast domain without requiring further authentication. In this case to access to the local network creates opportunities for both insiders and external attackers to modify the function of the product and, by doing so, use the product as means for attacks on its network environment.
[RF-M-03]	Internal network traversal risk factor	This risk factor applies when management interfaces accept routed connections within organizational perimeters, as routable management interfaces enable lateral movement attacks. As this risk factor is only applicable when organizational perimeters exist, it is of less relevance for devices for non-professional use as described in clause 4.7.2.1.
[RF-M-04]	Global internet exposure risk factor	This risk factor applies when management interfaces accept connections from public networks, as this increases the attack surface of the product especially when no additional authentication of such connections is required.
[RF-M-05]	Manual administration risk factor	This risk factor applies when devices support individual manual administration without network management system integration, as in this case both configuration and updates depend on the availability of the necessary personnel and are prone to human error and negligence.
[RF-M-06]	Centralized management compromise risk factor	This risk factor applies when devices support connection to network management systems or cloud platforms, as these centralized management systems can become single points of failure.

4299

4300 B.3.2.3 Protocol implementation risk factors

4301 The following risk factors arise from protocol implementations:

4302

Table B.7: Protocol implementation risk factors

ID	Title	Description
[RF-P-01]	Data transmission without encryption risk factor	This risk factor applies when devices support protocols that transmit data without encryption throughout the entire session, as the data can be easily accessed and manipulated during transmission.
[RF-P-02]	Request acceptance without authentication risk factor	This risk factor applies when devices implement protocols that accept requests without authentication, as this can lead to information being disclosed to illegitimate recipients or processing resources being illegitimately allocated and thereby no longer available for the products intended functionalities.
[RF-P-03]	Weak cryptography exploitation risk factor	This risk factor applies when devices support cryptographic algorithms or implementations thereof that are not state of the art, as this increases the success probability of attacks that are based on overcoming the cryptographic protection.
[RF-P-04]	Unverified trust establishment risk factor	This risk factor applies when devices implement protocols allow to make routing or security decisions without prior verification, as this enables illegitimate actors to manipulate packet processing rules and thereby the data flow within the affected network.
[RF-P-05]	Post-authentication cleartext risk factor	This risk factor applies when devices support protocols that protect authentication but transmit subsequent session data without encryption, as in this case access to an active session directly allows the extraction and manipulation of both data and commands.
[RF-P-06]	Cryptographic session compromise risk factor	This risk factor applies when implementing encrypted, authenticated protocols with any software stack, as implementation vulnerabilities can be prone to exploitation before patches or workarounds are available.

4303

4304 B.3.2.4 Data operations risk factors

4305 The following risk factors arise from data import/export operations:

4306

Table B.8: Data operations risk factors

ID	Title	Description
[RF-D-01]	Data transfer risk factor	This risk factor applies when the device supports data transfer, for example configuration backup and restore, log export, firmware upload, or any file import and export operations, as critical security parameters can be leaked or manipulated during transfer.

4307

4308 **B.3.3 Threat justification and mitigation**

4309 Table [B.9](#) lists, for each threat, the risk factors that contribute to its impact and likelihood, and the requirements of the
 4310 present document that mitigate it.

4311

Table B.9: Threat justification and mitigation

ID	Title	Contributing risk factor(s)	Requirement(s) for mitigation
[T-VH-01]	Exploitation of known vulnerabilities	[RF-B-01] [RF-M-05]	[REQ-KEV-1-02] [REQ-KEV-1-03] [REQ-UPDATE-1-01] [REQ-UPDATE-1-04] [REQ-UPDATE-1-05] [REQ-UPDATE-1-02] [REQ-UPDATE-1-06] [REQ-DEFAULT-1-08] [REQ-DEFAULT-1-09] [REQ-EXPOSURE-1-01] [REQ-EXPOSURE-1-02] [REQ-DEFAULT-1-07] [REQ-AVAIL-1-04]
[T-PS-01]	Interception of communication via the product	[RF-P-04]	[REQ-DEFAULT-1-08] [REQ-DATA-1-02] [REQ-DATA-1-04] [REQ-AUTH-2-04] [REQ-AUTH-4-01] [REQ-AUTH-4-04] [REQ-DEFAULT-1-07] [REQ-LOG-1-02] [REQ-TRANSFER-1-04]
[T-PS-02]	Redirection of communication to an illegitimate destination	[RF-P-04]	[REQ-PACKET-1-01] [REQ-AUTH-2-04] [REQ-AUTH-4-04] [REQ-DEFAULT-1-07] [REQ-LOG-1-02]
[T-PS-03]	Service limitation	[RF-B-03]	[REQ-AVAIL-1-01] [REQ-AVAIL-1-02] [REQ-DEFAULT-1-07] [REQ-AVAIL-1-04]
[T-PS-04]	Disruption of the availability of the product (DoS)	[RF-B-03] [RF-M-06] [RF-P-04]	[REQ-AUTH-2-04] [REQ-AUTH-4-02] [REQ-AUTH-4-04] [REQ-AVAIL-1-01] [REQ-AVAIL-1-02] [REQ-PACKET-1-01] [REQ-DEFAULT-1-07] [REQ-AVAIL-1-04]
[T-PS-05]	Resource exhaustion	[RF-B-03]	[REQ-AVAIL-1-01] [REQ-AVAIL-1-03] [REQ-PACKET-1-01] [REQ-DEFAULT-1-07] [REQ-AVAIL-1-04]

ID	Title	Contributing risk factor(s)	Requirement(s) for mitigation
[T-PS-06]	Deactivation of ancillary functionalities without authorization	[RF-B-03] [RF-M-01] [RF-M-02] [RF-M-03] [RF-M-04]	[REQ-DEFAULT-1-01] [REQ-DEFAULT-1-02] [REQ-AUTH-3-01] [REQ-AUTH-3-02] [REQ-AUTH-3-03] [REQ-AUTH-3-04] [REQ-AUTH-3-05] [REQ-AUTH-3-06] [REQ-DEFAULT-1-07] [REQ-LOG-1-02]
[T-PS-07]	Activation of ancillary functions without authorization	[RF-M-01] [RF-M-02] [RF-M-03] [RF-M-04]	[REQ-EXPOSURE-1-01] [REQ-AUTH-3-01] [REQ-AUTH-3-02] [REQ-AUTH-3-03] [REQ-AUTH-3-04] [REQ-AUTH-3-05] [REQ-AUTH-3-06] [REQ-DEFAULT-1-07] [REQ-LOG-1-02]
[T-AA-01]	Failure of access control	[RF-M-05] [RF-M-06]	[REQ-AUTH-1-01] [REQ-DEFAULT-1-05] [REQ-DEFAULT-1-06] [REQ-DEFAULT-1-07] [REQ-UPDATE-1-02] [REQ-AUTH-1-02] [REQ-AUTH-1-05] [REQ-AUTH-1-06] [REQ-AUTH-1-07] [REQ-AUTH-2-01] [REQ-AUTH-2-03] [REQ-INTEGRITY-1-04] [REQ-EXPOSURE-1-01] [REQ-TRANSFER-1-03] [REQ-TRANSFER-1-04] [REQ-LOG-1-03]
[T-AA-02]	Bypass authentication controls	[RF-P-02] [RF-P-03]	[REQ-DEFAULT-1-07] [REQ-DEFAULT-1-05] [REQ-DEFAULT-1-06] [REQ-AUTH-1-02] [REQ-AUTH-1-05] [REQ-AUTH-1-06] [REQ-AUTH-1-07] [REQ-AUTH-2-03] [REQ-AUTH-2-04] [REQ-AUTH-4-02] [REQ-AUTH-4-03] [REQ-AUTH-1-01] [REQ-INTEGRITY-1-04] [REQ-TRANSFER-1-03] [REQ-LOG-1-03]
[T-AA-03]	Brute force attack on user credentials	[RF-P-03]	[REQ-DEFAULT-1-07] [REQ-AUTH-1-05] [REQ-AUTH-1-06] [REQ-AUTH-2-04] [REQ-AUTH-4-03]
[T-AA-04]	Privilege escalation	[RF-P-06]	[REQ-DEFAULT-1-03] [REQ-DEFAULT-1-12] [REQ-AUTH-1-01] [REQ-AUTH-2-01] [REQ-AUTH-2-02]

ID	Title	Contributing risk factor(s)	Requirement(s) for mitigation
			[REQ-AUTH-2-03] [REQ-AUTH-2-04] [REQ-AUTH-3-05] [REQ-AUTH-3-06] [REQ-INTEGRITY-1-04] [REQ-DEFAULT-1-07] [REQ-LOG-1-02] [REQ-LOG-1-03]
[T-AA-05]	Session hijacking	[RF-P-06]	[REQ-DEFAULT-1-07] [REQ-AUTH-1-01] [REQ-AUTH-3-02] [REQ-AUTH-3-03] [REQ-AUTH-3-04] [REQ-AUTH-3-05] [REQ-LOG-1-02]
[T-TD-01]	Tampering physical components of the product	[RF-M-01]	[REQ-DEFAULT-1-05] [REQ-INTEGRITY-1-01] [REQ-DEFAULT-1-07] [REQ-INTEGRITY-1-03]
[T-TD-02]	Tampering of logical components of the product	[RF-B-06] [RF-M-01] [RF-M-02] [RF-M-03] [RF-M-04]	[REQ-DEFAULT-1-05] [REQ-AUTH-1-01] [REQ-AUTH-2-02] [REQ-AUTH-3-01] [REQ-AUTH-3-02] [REQ-AUTH-3-03] [REQ-AUTH-3-04] [REQ-AUTH-3-05] [REQ-AUTH-3-06] [REQ-AUTH-2-04] [REQ-EXPOSURE-1-01] [REQ-DEFAULT-1-07] [REQ-INTEGRITY-1-03]
[T-TD-03]	Tampering of data persistently stored on the product	[RF-P-02]	[REQ-RESET-1-02] [REQ-RESET-1-03] [REQ-AUTH-1-01] [REQ-AUTH-1-07] [REQ-AUTH-2-02] [REQ-AUTH-2-04] [REQ-AUTH-4-02] [REQ-DATA-1-02] [REQ-DATA-1-03] [REQ-DEFAULT-1-13] [REQ-DEFAULT-1-07] [REQ-LOG-1-03]
[T-TD-04]	Tampering of data processed and used by the product	[RF-P-02] [RF-P-05] [RF-P-06]	[REQ-AUTH-1-01] [REQ-AUTH-2-02] [REQ-AUTH-2-04] [REQ-AUTH-3-04] [REQ-AUTH-4-02] [REQ-DATA-1-02] [REQ-DATA-1-03] [REQ-INTEGRITY-1-01] [REQ-INTEGRITY-1-02] [REQ-INTEGRITY-1-03] [REQ-INTEGRITY-1-04] [REQ-PACKET-1-01] [REQ-LOG-1-03] [REQ-DEFAULT-1-07]
[T-TD-05]	Installation of tampered update packages	[RF-B-04]	[REQ-UPDATE-1-02] [REQ-UPDATE-1-06]

ID	Title	Contributing risk factor(s)	Requirement(s) for mitigation
			[REQ-UPDATE-1-07] [REQ-DEFAULT-1-13] [REQ-AUTH-1-01] [REQ-AUTH-2-02] [REQ-DATA-1-03] [REQ-INTEGRITY-1-01] [REQ-DEFAULT-1-07] [REQ-INTEGRITY-1-03]
[T-TD-06]	Disclosure without authorization of data processed or used by the product	[RF-B-02] [RF-P-01] [RF-P-02] [RF-D-01]	[REQ-RESET-1-01] [REQ-RESET-1-03] [REQ-AUTH-1-01] [REQ-AUTH-1-03] [REQ-AUTH-1-04] [REQ-AUTH-2-02] [REQ-AUTH-3-01] [REQ-AUTH-3-04] [REQ-AUTH-2-04] [REQ-AUTH-4-01] [REQ-AUTH-4-02] [REQ-AUTH-4-03] [REQ-DATA-1-02] [REQ-DATA-1-04] [REQ-TRANSFER-1-01] [REQ-TRANSFER-1-02] [REQ-TRANSFER-1-03] [REQ-TRANSFER-1-04] [REQ-DEFAULT-1-07] [REQ-LOG-1-02]

4312

4313

4314 Annex K (normative): 4315 Vertical specific state of the art cryptography

4316 K.1 General

4317 This annex provides additional vertical-specific generic requirements around the use of state of the art cryptography in
4318 routers, modems intended for the connection to the internet, and switches. It lists, by reference to the relevant normative
4319 clauses elsewhere in the present document, the cryptographic algorithm primitives, schemes and protocols that are
4320 commonly deployed on the market for these product categories and that are classified as CRY-SOTA for the purposes
4321 of the present document.

4322 K.1.1 Classification of cryptographic algorithms as CRY-SOTA

4323 For the purposes of the present document, a cryptographic algorithm, scheme or protocol is classified as CRY-SOTA
4324 where it is admitted under one of the ACM-listed or ACM-extended routes defined in items i), ii) or iii) below. A
4325 cryptographic algorithm, scheme or protocol that is not CRY-SOTA may nonetheless be used where it is admitted under
4326 the interoperability-based route defined in item iv) below.

4327 A cryptographic algorithm, scheme or protocol is CRY-SOTA where at least one of the following applies:

4328 i) ACM-listed: it is listed as Recommended (or equivalent) in the European Cybersecurity Certification Group's Agreed
4329 Cryptographic Mechanisms catalogue (ACM) [\[4\]](#);

4330 ii) ACM-extended (recognized catalogue): it is not listed in the ACM, and it is listed as Recommended (or equivalent),
4331 and is not marked as deprecated, legacy-only or disallowed at the time of the conformity assessment, in any of the
4332 following recognized public cryptographic catalogues:

- 4333 • NIST publications in the Special Publication 800 series, the FIPS series, and the associated CAVP/ACVP test-
4334 vector programmes;
- 4335 • BSI TR-02102 series [\[5\]](#);
- 4336 • ANSSI Référentiel Général de Sécurité, Annex B2 [\[6\]](#);
- 4337 • CCCS ITSP.40.062 [\[7\]](#);
- 4338 • a sector-specific cryptographic algorithm catalogue maintained by a recognized standards-development
4339 organization (see EXAMPLE 2);

4340 iii) ACM-extended (vertical content): it is listed in the normative cryptographic content of the present document for
4341 routers, modems and switches (see clauses [K.3](#) through [K.8](#)).

4342 A cryptographic algorithm, scheme or protocol that is not CRY-SOTA under items i), ii) or iii) may be used only as
4343 follows:

4344 iv) Interoperability-based: it is required for a specific product function to comply with a well-defined external
4345 specification or external requirement, and its use meets all of the conditions for legacy interoperability set out in clause
4346 [K.2.4](#) (2). Inclusion of a cryptographic algorithm, scheme or protocol under this route does not classify it as CRY-
4347 SOTA.

4348 NOTE 1: Items i), ii) and iii) are listed as alternatives for classification as CRY-SOTA. A manufacturer is not
4349 required to demonstrate classification under more than one of these items for the same algorithm. Item iv)
4350 is not a CRY-SOTA classification; it admits a non-CRY-SOTA algorithm under controlled
4351 interoperability conditions.

4352 NOTE 2: Where two recognized catalogues classify the same algorithm differently, the manufacturer should rely on
4353 whichever produces the more conservative (less permissive) classification.

4354 NOTE 3: A cryptographic mechanism composed of more than one cryptographic primitive (for example a hybrid
4355 key-encapsulation mechanism or a hybrid signature scheme) inherits the most restrictive classification of
4356 its constituent primitives. A hybrid construction including a Legacy or Deprecated component is therefore
4357 classified as Legacy or Deprecated, regardless of the classification of the other components.

4358 NOTE 4: In item iv), an external specification or external requirement means a specification or requirement that is
 4359 imposed on the product and that requires the use of a specific cryptographic algorithm, scheme or
 4360 protocol for the product to interoperate with an identified system, platform or operational context. An
 4361 external requirement can be, for instance, a regulatory requirement, an operational constraint, a technical
 4362 interoperability constraint, or a platform compatibility requirement.

4363 NOTE 5: The routes in items i) to iv) correspond to the ACM-listed, ACM-extended and interoperability-based
 4364 cryptographic mechanism routes of the cross-vertical Annex K framework. Items i) to iii) correspond to
 4365 the ACM-listed and ACM-extended routes; item iv) corresponds to the interoperability-based route, the
 4366 conditions of which are specified for the present document in clause [K.2.4](#) (2).

4367 K.2 Assessment criteria for compliance with cryptographic 4368 requirements

4369 K.2.1 Assessment objective

4370 The purpose of this assessment case is to verify that, for every cryptographic algorithm, scheme or protocol used by a
 4371 security mechanism of the product, appropriate evidence is provided demonstrating classification as CRY-SOTA in
 4372 accordance with clause [K.1](#), by reference to one of paths i), ii) or iii) of that clause.

4373 K.2.2 Assessment preparation

4374 Preconditions for the assessment:

- 4375 • where the product has a default configuration, that default configuration shall be used for the assessment;
- 4376 • otherwise, the delivery-state configuration shall be used (i.e. the configuration of the product as made available
 4377 on the market in accordance with Annex I, Part I, point (2)(b) of Regulation (EU) 2024/2847 [\[i.1\]](#));
- 4378 • the manufacturer shall make available a list identifying every security mechanism of the product, the
 4379 cryptographic algorithm, scheme or protocol used by that mechanism, the parameters in use, and whether the
 4380 algorithm forms part of the default or delivery-state configuration.

4381 K.2.3 Assessment activities

4382 For every security mechanism identified under the preceding clause, the assessor shall:

- 4383 1) review the documentation provided and confirm that, for each algorithm in use, the manufacturer has identified the
 4384 path of clause [K.1](#) (i, ii, or iii) by which the algorithm is classified as CRY-SOTA, and the corresponding catalogue
 4385 entry or clause reference;
- 4386 2) verify that the catalogue entry or clause reference cited under (1) exists, is published, and is not marked as
 4387 deprecated, legacy-only or disallowed at the time of the assessment;
- 4388 3) inspect the product in the configuration identified under the preceding clause and confirm that the cryptographic
 4389 algorithm and parameters in use match the documented configuration;
- 4390 4) where the manufacturer has documented the use of an algorithm that is not classified as CRY-SOTA under any path
 4391 of clause [K.1](#), verify that the conditions for legacy interoperability are met.

4392 K.2.4 Assessment evidence

- 4393 1) For each cryptographic algorithm in use, a reference to a publicly available catalogue entry or to the relevant clause
 4394 of the present document, in accordance with one of the paths of clause [K.1](#). Acceptable references include:
 - 4395 a) the entry in the ACM catalogue (path i);
 - 4396 b) the entry in any of the recognized catalogues listed under [K.1.1](#) (ii) (path ii); for example a national cryptographic
 4397 catalogue published by a Member State authority, a sector-specific catalogue published by a recognized standards-
 4398 development organization, or an industry catalogue, where the catalogue is publicly available and is maintained under a
 4399 documented revision and retirement process;
 - 4400 c) the clause of the present document listing the algorithm as part of the vertical-specific cryptographic content for
 4401 routers, modems and switches (path iii);

- 4402 d) where an algorithm is referenced under path ii) or path iii) but is not present in the ACM, the documentation shall in
 4403 addition identify the publicly available specification (e.g. an IETF Request for Comments, an IEEE standard, an ETSI
 4404 deliverable, a NIST publication) under which the algorithm is implemented.
- 4405 2) Where a non-CRY-SOTA algorithm is offered by the product to support interoperability with a specifically identified
 4406 legacy system, in accordance with recital (55) of Regulation (EU) 2024/2847 [i.1] and section 2.5 of the Commission
 4407 Guidance on its application, the documentation shall demonstrate that all of the following conditions are met:
- 4408 a) the non-CRY-SOTA algorithm is not used in the default or delivery-state configuration;
- 4409 b) where the relevant security mechanism supports algorithm negotiation, a CRY-SOTA algorithm is offered and is
 4410 preferred over the non-CRY-SOTA algorithm during negotiation;
- 4411 c) the documentation identifies the specific legacy system or systems for which the non-CRY-SOTA algorithm is
 4412 required, and the legacy constraint that prevents use of a CRY-SOTA alternative;
- 4413 d) the documentation declares a sunset date for the non-CRY-SOTA algorithm that falls within the declared intended
 4414 lifetime of the product;
- 4415 e) a user-facing indication (such as a log entry, a management-interface warning, or an equivalent mechanism) informs
 4416 an administrator when the non-CRY-SOTA algorithm is in use.
- 4417 3) As a supplemental verification, not sufficient on its own, the manufacturer shall identify whether any entry in the
 4418 ENISA European Vulnerability Database (EUVD) [i.14], in the Single Reporting Platform (SRP) [i.15] established
 4419 under Regulation (EU) 2024/2847 [i.1], or in equivalent publicly accessible cryptanalytic literature, identifies a
 4420 fundamental cryptanalytic break of the algorithm in use (as distinct from an implementation defect in a specific
 4421 product). Where such a break is identified, the algorithm shall not be classified as CRY-SOTA notwithstanding any
 4422 catalogue listing.
- 4423 4) Where the catalogue referenced under path ii) does not provide a lifecycle classification, the manufacturer shall
 4424 document the algorithm's expected deprecation date based on the published cryptanalytic state of the art.
- 4425 NOTE 1: The ACM catalogue references a number of cryptographic specifications published as ISO/IEC standards.
 4426 Where such referenced specifications exist, technically equivalent specifications published in publicly
 4427 available form (for example as IETF RFCs, as NIST Special Publications, or as IEEE standards) can also
 4428 be cited as evidence under path ii) of clause K.1.
- 4429 NOTE 2: The reference catalogues identified under K.1.1 (ii) use a range of lifecycle terminologies (for example
 4430 "Recommended" / "Legacy" / "Deprecated" in the ACM; "Acceptable" / "Disallowed" in NIST SP 800-
 4431 131A [8]; "Recommended" / "Legacy use" in BSI TR-02102-1 [5]).
- 4432 NOTE 3: The supplemental check under (3) above is intended to capture the case where a cryptographic primitive
 4433 listed in a catalogue is nevertheless subject to a fundamental break that has not yet been reflected in
 4434 catalogue revisions. Vulnerability database entries typically catalogue implementation defects in specific
 4435 products, which are not in themselves a basis for declassifying an algorithm.

4436 K.2.5 Assessment verdict

4437 The verdict pass shall be assigned where, for every cryptographic algorithm, scheme or protocol identified under the
 4438 assessment preparation:

- 4439 1) evidence has been provided classifying the algorithm as CRY-SOTA under one of the paths of clause K.1;
- 4440 2) inspection has confirmed that the documented configuration is the active configuration of the product;
- 4441 3) where applicable, the conditions for legacy interoperability have been verified; and
- 4442 4) the supplemental cryptanalytic-status check has not identified a disqualifying entry.

4443 The verdict fail shall be assigned otherwise.

4444 EXAMPLE 1: A national cryptographic catalogue under K.1.1 (ii) is BSI TR-02102-1 [5], Cryptographic
 4445 Mechanisms: Recommendations and Key Lengths, version 2026-01, 31 January 2026, published by the
 4446 Federal Office for Information Security (Germany). It is also an example of a national catalogue
 4447 referenced from the ACM.

4448 EXAMPLE 2: Sector-specific cryptographic catalogues published by recognized standards-development
 4449 organizations under K.1.1 (ii) include:

- 4450
- ETSI TS 119 312 [9], Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites;
- 4451
- ETSI TS 133 210 [10], Network Domain Security (NDS); IP network layer security (relevant to operator-managed router and modem deployments);
- 4452
- IETF cryptographic specifications published as Standards-Track or Best-Current-Practice RFCs, where the specification is referenced by a recognized national or sector catalogue.
- 4453
- 4454

4455 EXAMPLE 3: An industry-relevant cryptographic catalogue example for routers, modems and switches is the
 4456 Canadian Centre for Cyber Security ITSP.40.062 [7], Guidance on Securely Configuring Network
 4457 Protocols, which provides parameter-level guidance for TLS, IPsec, SSH, and other protocols typical of
 4458 the present document's product scope.

4459 NOTE 1: Vertical-Standard-specific evidence for the appropriateness of a cryptographic algorithm can be added by
 4460 the present document under path iii) of clause K.1. Examples of such evidence include a description and
 4461 formal verification, a cryptographic security proof, a security analysis of a new algorithm, or a side-
 4462 channel analysis.

4463 NOTE 2: Formal verification, where used, employs mathematical proofs or rigorous methods to demonstrate that an
 4464 algorithm meets its formal specification for all valid inputs, in contrast with testing, which samples
 4465 specific cases.

4466 NOTE 3: A hybrid cryptographic construction (for example a hybrid key-encapsulation mechanism or a hybrid
 4467 signature scheme) inherits the most restrictive classification of its constituent primitives. Hybrid
 4468 constructions are therefore not a general strategy for mitigating the deprecation of a constituent algorithm.
 4469 Where a hybrid is used as part of the migration to post-quantum cryptography, the construction should be
 4470 implemented in a way that allows the classical component to be cleanly removed once the post-quantum
 4471 component is independently sufficient.

4472 K.3 Symmetric atomic primitives

4473 K.3.1 Block ciphers

4474 No additional primitives.

4475 K.3.2 Stream ciphers

4476 Block ciphers can be configured to behave like stream ciphers using counter (CTR) mode, as described in the ACM
 4477 catalogue clause 3.1. In addition, the stream ciphers included in Table K.1 are agreed as state of the art.

4478 **Table K.1: State of the art stream ciphers.**

Primitive	Parameter's sizes	Notes
ChaCha20 (RFC 8439 [11])	256 bit (key)	A modern stream cipher used in VPNs and TLS 1.3. Preferred for devices without AES hardware acceleration. Extending ChaCha20 with a larger 24-byte nonce (XChaCha20) to mitigate nonce collisions is included in this primitive.

4479

4480 K.3.3 Hash functions

4481 No additional primitives.

4482 K.4 Symmetric constructions

4483 K.4.1 Confidentiality modes of operation: encryption/decryption modes

4484 No additional schemes.

4485 K.4.2 Specific confidentiality modes: disk encryption

4486 No additional schemes.

4487 K.4.3 Integrity modes: message authentication codes

4488 The additional message authentication codes included in Table [K.2](#) are agreed as state of the art.

4489 **Table K.2: State of the art message authentication codes.**

Scheme	Parameter's sizes	Notes
Poly1305 (IETF RFC 8439 [11])	128 (tag)	Paired with ChaCha20 in TLS 1.3.
UMAC (IETF RFC 4418 [12])	128	Used in SSH configurations for managing switches and routers.

4490

4491 K.4.4 Symmetric entity authentication schemes

4492 The additional symmetric entity authentication schemes included in Table [K.3](#) are agreed as state of the art.

4493 **Table K.3: State of the art symmetric entity authentication schemes.**

Scheme	Parameter's sizes	Notes
AES-CMAC	128	IEEE 802.11w Protected Management Frames.

4494

4495 K.4.5 Authenticated encryption

4496 The additional authentication encryption schemes included in Table [K.4](#) are agreed as state of the art.

4497 **Table K.4: State of the art authentication encryption schemes.**

Scheme	Parameter's sizes	Notes
ChaCha20-Poly1305 (RFC 8439 [11])	256 bit (key)	Standard AEAD for TLS 1.3. Extending ChaCha20 with a larger 24-byte nonce (XChaCha20) to mitigate nonce collisions is included in this primitive.

4498

4499 K.4.6 Key protection

4500 No additional schemes.

4501 K.4.7 Key derivation functions

4502 The additional key derivation functions included in Table [K.5](#) are agreed as state of the art.

4503 **Table K.5: State of the art key derivation functions.**

Scheme	Parameter's sizes	Notes
IEEE 802.11 Pseudo-Random Function (PRF), as defined in Clause 12.7.1.2 of IEEE 802.11-2020 [13]	128 / 256 / 384 / 512 / 704	Mandatory for WPA2/WPA3 session key derivation.

4504

4505 K.4.8 Password protection/password hashing mechanisms

4506 The additional password protection / password hashing mechanisms included in Table [K.6](#) are agreed as state of the art.

4507 Every password-based hashing mechanism shall include a unique random salt (at least 16 bytes) per user.

4508

Table K.6: State of the art password protection / password hashing mechanisms.

Primitive	Parameter's sizes	Notes
Argon2id (IETF RFC 9106 [14])	Output: 32 bytes, OpsLimit: 2, Memory: 19 MiB, Threads: 1 (or higher)	A resource intensive hash function to protect passwords. Can also be used as a KDF to derive secret keys from passwords. Generated entropy depends on the entropy of the password.
Scrypt (IETF RFC 7914 [15])	Cost: 2^{17} , block size 1024 bytes, parallelization 1 (or higher)	A resource intensive hash function to protect passwords. Can also be used as a KDF to derive secret keys from passwords. Generated entropy depends on the entropy of the password.

4509

4510 K.4.9 Key combiners

4511 The additional key combining schemes included in Table [K.7](#) are agreed as state of the art.

4512

Table K.7: State of the art key combining schemes.

Scheme	Parameter's sizes	Notes
IEEE 802.11r KDF	256	Derives PMK-R1 from PMK-R0 for fast Wi-Fi roaming.
ERP KDF (RFC 5295 [16])	512	Used in 802.11ai (FILS) for rapid Wi-Fi re-authentication.

4513

4514 K.5 Asymmetric atomic primitives

4515 K.5.1 RSA/Integer factorization

4516 No additional primitives.

4517 K.5.2 Discrete logarithm in finite fields

4518 No additional primitives.

4519 K.5.3 Discrete logarithm in elliptic curves

4520 The additional elliptic curve parameters included in Table [K.8](#) are agreed as state of the art.

4521

Table K.8: Additional elliptic curve parameters agreed as state of the art.

Scheme	Curve	Notes
X25519 / Ed25519 (RFC 8410 [17])	Curve25519	Standard for TLS 1.3, and SSH.
X448 / Ed448 (RFC 8410 [17])	Curve448	High-security (224-bit security) IETF standard.

4522

4523 K.5.4 Learning with errors in (structured) lattices

4524 No additional LWE mechanisms.

4525 K.5.5 Hash function preimage resistance

4526 The additional schemes included in Table [K.9](#) are agreed as state of the art.

4527

Table K.9: State of the art hash function schemes.

Scheme	Parameter's sizes	Notes
Hash-to-Element (H2E, as specified in clause 12.4.3.5 of IEEE 802.11-2020 [13])	256 / 384	Mandatory for WPA3 to prevent side-channel attacks.
SAE-PK, as specified in clause 12.4.9 of IEEE 802.11-2020 [13]	256	WPA3 enhancement to prevent AP impersonation.

4528

4529 **K.5.6 Other intractable problems**

4530 No additional schemes.

4531 **K.6 Asymmetric constructions**4532 **K.6.1 Asymmetric encryption scheme**

4533 No additional schemes.

4534 **K.6.2 Digital signature**

4535 The additional digital signature schemes included in Table K.10 are agreed as state of the art.

4536

Table K.10: State of the art digital signature schemes.

Scheme	Parameter's sizes	Notes
Ed25519 (RFC 8032 [18])	256 bit key	Used for TLS and formally known as EdDSA.

4537

4538 **K.6.3 Asymmetric entity authentication schemes**

4539 The additional asymmetric entity authentication schemes included in Table K.11 are agreed as state of the art.

4540

Table K.11: State of the art entity authentication schemes.

Scheme	Parameter's sizes	Notes
Ed25519-256 with Curve25519 (RFC 8420 [19])	256 bit	
EAP-TLS (IEEE 802.1X)	ECDSA: 255-bit / RSA: 2048-bit	
SAE-PK, see clause 12.4.8.6 of IEEE 802.11-2020 [13]	NIST P-256	WPA3-Personal enhancement.
OWE, see clause 12.12.2 of IEEE 802.11-2020 [13] and RFC 8110 [20]	P-256	Wi-Fi Enhanced Open (Encryption for public hotspots).
DPP (Wi-Fi Alliance, "Easy Connect Specification" [21])	P-256	Wi-Fi Easy Connect (IoT onboarding).

4541

4542 **K.6.4 Key establishment and key encapsulation**

4543 The additional key establishment and key encapsulation schemes included in Table K.12 are agreed as state of the art.

4544

Table K.12: State of the art key establishment and key encapsulation primitives.

Primitive	Scheme	Notes
EC-DLOG, see clause 12.4.8.2 of IEEE 802.11-2020 [13]	SAE (Simultaneous Authentication of Equals)	The mandatory handshake for WPA3-Personal.
EC-DLOG, see clause 12.4.8.2 of IEEE 802.11-2020 [13]	ECDH (Elliptic Curve Diffie-Hellman)	

4545

4546 K.7 Cryptographic protocols

4547 K.7.1 QUIC

4548 The QUIC protocol included in Table [K.13](#) is agreed as state of the art.

4549 **Table K.13: Additional QUIC protocol agreed as state of the art.**

QUIC Protocol Version
QUIC version 1 (RFC 9000 [22])

4550

4551 The QUIC cipher suites included in Table [K.14](#) are agreed as state of the art.

4552 **Table K.14: QUIC cipher suites agreed as state of the art.**

Hex Code	Cipher Suite	Notes
0x1301	TLS AES 128 GCM SHA256	
0x1302	TLS AES 256 GCM SHA384	
0x1303	TLS CHACHA20 POLY1305 SHA256	
0x1304	TLS AES 128 CCM SHA256	

4553

4554 K.7.2 MACSec

4555 The MACSec protocols included in Table [K.15](#) are agreed as state of the art.

4556 **Table K.15: MACSec protocol agreed as state of the art.**

MACSec Protocol Version
IEEE 802.1AE [23]

4557

4558 The MACSec cipher suites included in Table [K.16](#) are agreed as state of the art.

4559 **Table K.16: MACSec cipher suites agreed as state of the art.**

Algorithm Name	Notes
GCM-AES-XPB-256	
GCM-AES-256	
GCM-AES-XPB-128	

4560

4561 K.7.3 SNMP

4562 The SNMP protocols included in Table [K.17](#) are agreed as state of the art.

4563 **Table K.17: SNMP protocol agreed as state of the art.**

SNMP Protocol Version
SNMPv3 (RFC 3411 [24] , RFC 3412 [25])

4564

4565 The SNMPv3 cipher suites included in Table [K.18](#) are agreed as state of the art.

4566 **Table K.18: SNMPv3 cipher suites agreed as state of the art.**

Algorithm Name	Notes
AES-256-CFB	
AES-128-CFB	

4567

4568 K.7.4 Routing protocols

4569 The routing protocols included in Table [K.19](#) are agreed as state of the art.

4570 **Table K.19: Routing protocols agreed as state of the art.**

Protocol Version
BGPsec (IETF RFC 8205 [26])
OSPFv2 (IETF RFC 5709 [27])
OSPFv3 (IETF RFC 7166 [28])
IS-IS (IETF RFC 5310 [29])
BGP (authenticated using IETF RFC 5925 [30])

4571

4572 The routing protocol algorithms included in Table K.20 are agreed as state of the art.

4573 **Table K.20: Routing protocol algorithms agreed as state of the art.**

Group	Algorithm Name	Notes
BGPsec	ECDSA P-256/SHA-256	Used to sign the AS_PATH at every hop.
OSPF	HMAC-SHA-256	
OSPF	HMAC-SHA-384	
OSPF	HMAC-SHA-512	
IS-IS	HMAC-SHA-256	
IS-IS	HMAC-SHA-384	
IS-IS	HMAC-SHA-512	
BGP	AES-128-CMAC	

4574

4575

K.7.5 Secure device identity

4576 The secure device identity protocols included in Table K.21 are agreed as state of the art.

4577 **Table K.21: Secure device identity protocols agreed as state of the art.**

Secure Device Identity
IEEE 802.1AR [31]

4578

4579 The cipher suites used with secure device identity protocols included in Table K.22 are agreed as state of the art.

4580 **Table K.22: Secure device identity cipher suites agreed as state of the art.**

Algorithm Name	Notes
P-256	
P-384	

4581

4582

K.7.6 Time Protocols

4583 The time protocols included in Table K.23 are agreed as state of the art.

4584 **Table K.23: Time protocol agreed as state of the art.**

Time Protocol
IEEE 1588-2019 [32]
NTS-Authenticated NTP (IETF RFC 8915 [33])

4585

4586 The cipher suites included in Table K.24 are agreed as state of the art for use with the time protocols.

4587 **Table K.24: Time protocol cipher suites agreed as state of the art.**

Group	Algorithm Name	Notes
IEEE 1588 PTP AUTHENTICATION TLV (Annex P of IEEE 1588 [32])	HMAC-SHA256-128	

Group	Algorithm Name	Notes
IEEE 1588 PTP AUTHENTICATION TLV	AES-GMAC	
IEEE 1588 PTP AUTHENTICATION TLV	HMAC-SHA256	
IEEE 1588 PTP AUTHENTICATION TLV	HMAC-SHA512	
NTS AEAD Integrity Algorithm	AES-SIV	Mandatory AEAD for Secure Network Time (RFC 8915 [33]).

4588

4589 K.8 Cryptographic industry standards

4590 The following industry standards serve as a baseline for approved cryptographic algorithms and are considered
4591 approved as CRY-SOTA. The standards listed in Table [K.25](#) are agreed as state of the art.

4592

Table K.25: National catalogues defined as CRY-SOTA.

Cryptographic Mechanisms	Version	Notes
BSI TR-02102-1 [5]	2026-01	
BSI TR-02102-2 [34]	2026-01	
BSI TR-02102-3 [35]	2026-01	
BSI TR-02102-4 [36]	2026-01	

4593

4594 K.9 Crypto agility

4595 K.9.1 Requirement

4596 Where the product's default configuration uses a cryptographic mechanism for which the ACM catalogue, or the
4597 present document, specifies a deprecation date, expiry date, migration condition or usage limitation falling within the
4598 intended lifetime of the product, the product shall provide means for addressing the affected cryptographic mechanism
4599 by one or more of the following:

- 4600 a) updating the cryptographic mechanism;
- 4601 b) using another cryptographic mechanism that complies with clause [K.1.1](#) and is not subject to the relevant deprecation
4602 date, expiry date, migration condition or usage limitation;
- 4603 c) disabling the use of the affected cryptographic mechanism; or
- 4604 d) limiting the use of the affected product functions accordingly.

4605 **EXAMPLE 1:** Where a security mechanism uses a hybrid cryptographic construction, for example a hybrid key-
4606 encapsulation mechanism combining a classical and a post-quantum primitive, the lifecycle status of each
4607 constituent primitive is relevant to the lifecycle status of the construction. Hybridization can be used as
4608 part of a planned migration strategy where permitted by the ACM catalogue or by the present document.
4609 However, hybridization does not, by itself, extend the recommended usage lifetime of a constituent
4610 primitive that has been deprecated.

4611 **NOTE 1:** Where a hybrid cryptographic construction includes multiple cryptographic primitives, the lifecycle status
4612 of each constituent primitive is relevant to the lifecycle status of the construction. Hybridization is not
4613 assumed to mitigate the deprecation of a constituent primitive unless the ACM catalogue or the present
4614 document classifies the hybrid construction as suitable for the corresponding product function.

4615 **NOTE 2:** Crypto agility supports maintaining appropriate cryptographic protection within the intended lifetime of
4616 the product, in addition to the capability of updating cryptographic mechanisms on the product in
4617 accordance with secure update and secure communication mechanisms.

4618 **NOTE 3:** Deprecation information from sources other than the ACM catalogue or the present document can be
4619 considered as input to vulnerability management or security risk assessment but does not by itself trigger
4620 the requirement in clause [K.9.1](#).

4621 NOTE 4: Where the product provides cryptographic capabilities for use by other products, components or layers,
 4622 the mechanism required by clause [K.9.1](#) can consist of update, configuration, disabling, deprecation or
 4623 limitation capabilities usable by the integrating product, system operator or user, where applicable.

4624 NOTE 5: The applicability condition of this requirement can express exceptions based on product characteristics,
 4625 e.g. cryptographic implementation based on immutable hardware co-processor(s) or hardware-based root
 4626 of trust, or long-lived silicon used in a long-lived non-updateable environment.

4627 K.9.2 Assessment of crypto-agility

4628 K.9.2.1 Assessment objective

4629 The purpose of this assessment case is to verify whether, where the product's default configuration uses a cryptographic
 4630 mechanism for which the ACM catalogue, or the present document, specifies a deprecation date, expiry date, migration
 4631 condition or usage limitation falling within the intended lifetime of the product, the product provides means to address
 4632 the affected cryptographic mechanism in accordance with clause [K.9.1](#).

4633 K.9.2.2 Assessment preparation

4634 • Preconditions for the assessment: The product's default configuration shall be used for the assessment.

4635 • The documentation shall identify:

4636 a) the intended lifetime of the product;

4637 b) the cryptographic mechanisms used in the product's default configuration;

4638 c) the related product function(s) for each cryptographic mechanism;

4639 d) the lifecycle information applicable to each cryptographic mechanism, where specified by the ACM catalogue or the
 4640 present document, including any deprecation date, expiry date, migration condition or usage limitation.

4641 K.9.2.3 Assessment activities

4642 The assessment shall include verification that:

4643 a) for each cryptographic mechanism used in the product's default configuration, the lifecycle information specified by
 4644 the ACM catalogue or the present document has been identified, where such information is specified;

4645 b) where the ACM catalogue or the present document specifies a deprecation date, expiry date, migration condition or
 4646 usage limitation for a cryptographic mechanism, this information is reflected in the documentation;

4647 c) where a deprecation date, expiry date, migration condition or usage limitation falls within the intended lifetime of the
 4648 product, the product provides an applicable mechanism for updating the cryptographic mechanism, using another
 4649 cryptographic mechanism that complies with clause [K.1.1](#) and is not subject to the relevant deprecation date, expiry
 4650 date, migration condition or usage limitation, disabling the use of the affected cryptographic mechanism, or limiting the
 4651 use of the affected product functions accordingly;

4652 d) where another cryptographic mechanism is used, that cryptographic mechanism complies with clause [K.1.1](#) and is
 4653 not subject to the relevant deprecation date, expiry date, migration condition or usage limitation.

4654 K.9.2.4 Assessment evidence

4655 The assessment evidence shall include, as applicable:

4656 a) documentation of the intended lifetime of the product;

4657 b) list of cryptographic mechanisms used in the product's default configuration;

4658 c) identification of the related product function(s) for each cryptographic mechanism;

4659 d) references to the ACM catalogue entry or to the provision of the present document used to determine lifecycle
 4660 information, where applicable;

4661 e) identification of any deprecation date, expiry date, migration condition or usage limitation falling within the intended
 4662 lifetime of the product;

4663 f) description of the means provided by the product, such as update of the cryptographic mechanism, use of another
4664 cryptographic mechanism that complies with clause [K.1.1](#) and is not subject to the relevant lifecycle constraint,
4665 disabling the use of the affected cryptographic mechanism, or limitation of the use of the affected product functions.

4666 K.9.2.5 Assessment verdict

- 4667 • The verdict PASS shall be assigned if the required evidence has been provided, is complete, is applicable to
4668 the assessed configuration, and demonstrates compliance.