



Cyber Security (CYBER); Cyber Resilience Act (CRA); Cybersecurity requirements for smart home products with security functionalities

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 304 631 Smart home assistants · 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**.

Reference

< DEN/CYBER-EUS-0014 >

Keywords

< CRA;Cybersecurity;intelligent homes & buildings
>

0

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

Reproduction is only permitted for the purpose of standardization work undertaken within ETSI.
The copyright and the foregoing restrictions extend to reproduction in all media.

© ETSI 2026.
All rights reserved.

Contents

1			
2			
3	Intellectual Property Rights		7
4	Foreword.....		7
5	Modal verbs terminology		8
6	1 Scope		9
7	2 References		9
8	2.1 Normative references		9
9	2.2 Informative references		9
10	3 Definition of terms, symbols and abbreviations.....		10
11	3.1 Terms		10
12	3.2 Abbreviations.....		17
13	4 Product context.....		18
14	4.1 Product functions		18
15	4.1.1 Residential physical security function.....		18
16	4.1.2 Supporting functions		19
17	4.1.3 Data assets.....		20
18	4.2 Product Architecture.....		20
19	4.3 Operational Environment.....		21
20	4.4 Interfaces.....		22
21	4.5 Distribution of security functions		22
22	4.6 Users		22
23	4.7 Use cases.....		23
24	4.7.1 General		23
25	4.7.2 Use case profiles		23
26	4.8 Security Profiles.....		23
27	5 Requirements specifications.....		24
28	5.1 Product's technical requirements specifications.....		24
29	5.1.1 Known exploitable vulnerabilities.....		24
30	5.1.1.1 [NKEV-MKAV] No known exploitable vulnerabilities.....		25
31	5.1.1.2 [NKEV-SUM-SUPPORT] Secure software update mechanism.....		25
32	5.1.1.3 [NKEV-SUM-PROVIDE] Secure software update mechanism for core components		25
33	5.1.1.4 [NKEV-SUM-AUTO] Automated security updates.....		25
34	5.1.1.5 [NKEV-SUM-NOTIF] Update notifications		25
35	5.1.2 Default configuration		25
36	5.1.2.1 [SDC-AUM-FH] Default configuration of authentication for functions whose use can cause harm ...		25
37	5.1.2.2 [SDC-SUM-AUTO] Default configuration of automated security updates.....		25
38	5.1.2.3 [SDC-SUM-NOTIF] Default configuration of update notifications.....		26
39	5.1.2.4 [SDC-FRM] Factory reset to restore the default state		26
40	5.1.3 Authentication and access control mechanisms		26
41	5.1.3.1 [ACM-FH] Access control for functions whose use can cause harm.....		26
42	5.1.3.2 [AUM-FH] Authentication for functions whose use can cause harm.....		26
43	5.1.3.3 [AUTHZ-LP] Least privilege in authorization policies.....		27
44	5.1.3.4 [AUTHZ-R] Revocability of granted permissions		27
45	5.1.4 Integrity protection.....		27
46	5.1.4.1 [INT-SWPCK] Software package verification		27
47	5.1.4.2 [INT-COM] Communication of integrity relevant data.....		28
48	5.1.5 Confidentiality protection		28
49	5.1.5.1 [CONF-SSM] Confidentiality protecting persistent storage for confidential data		28
50	5.1.5.2 [CONF-COM] Communication of confidential data.....		28
51	5.1.6 Data minimization		29
52	5.1.6.1 [DMIN-DJST] Documented justification of processed data.....		29
53	5.1.7 Availability protection.....		29

54	5.1.7.1	[AVAI-TIME-RECO-POW] Restoration after loss of power	29
55	5.1.7.2	[AVAI-TIME-NETW] Local operation.....	29
56	5.1.7.3	[AVAI-TIME-RECO-NETW] Restoration after loss of network connection	29
57	5.1.7.4	[AVAI-TIME-OUTA-NOT] Notify non-availability	29
58	5.1.7.5	[AVAI-TIME-PREV-NOT] Notify upcoming limitation.....	29
59	5.1.7.6	[AVAI-TIME-NET-PRIO] Network prioritization	30
60	5.1.7.7	[AVAI-TIME-RES-PRIO] Power resource prioritization	30
61	5.1.7.8	[AVAI-TIME-IMP-AMP] Amplification control.....	30
62	5.1.7.9	[AVAI-TIME-DOS-RATE] Incoming rate limiting.....	30
63	5.1.7.10	[AVAI-SUM-SCHEDULE] Scheduling of updates	30
64	5.1.8	Impact minimization	30
65	5.1.9	Limit attack surface.....	30
66	5.1.9.1	[LAS-INVAL] Validation of external data input.....	30
67	5.1.9.2	[LAS-INSAN] Sanitization of external data input.....	31
68	5.1.9.3	[LAS-PHY-INF] Only necessary physical interfaces.....	31
69	5.1.9.4	[LAS-LOGIC-INF] Only necessary logical interfaces active by default.....	31
70	5.1.9.5	[LAS-APP] Only necessary apps by default.....	31
71	5.1.9.6	[LAS-SBOOT] Secure boot.....	31
72	5.1.10	Logging and monitoring mechanisms	31
73	5.1.10.1	[LOG-LOW] Events to log for low risk SHPSF.....	31
74	5.1.10.2	[LOG-MEDIUM] Events to log for medium risk SHPSF	31
75	5.1.10.3	[LOG-HIGH] Events to log for high risk SHPSF.....	32
76	5.1.10.4	[LOG-TIME] Timestamps for logs	32
77	5.1.10.5	[LOG-TIME-HIGH] Real-Timestamps for logs.....	32
78	5.1.10.6	[LOG-STORAGE] Persistently store logfiles	32
79	5.1.10.7	[LOG-BACKUP] Backup of logfiles	32
80	5.1.11	Deletion mechanisms	32
81	5.1.11.1	[DLM-PERM] Permanent removal of user-related data.....	32
82	5.1.12	Other product's technical requirements specifications	33
83	5.1.12.1	[USERNOT-NOSECFCUC] User notifications on not available security functions.....	33
84	5.1.12.2	[USERNOT-SECREL] Language and representation for security-related user notifications	33
85	5.1.12.3	[GUI-SECCONF] Visual representation of security-related configuration via GUIs	33
86	5.1.12.4	[CRY-SOTA] State-of-the-art cryptography	33
87	5.1.12.5	[CRY-CCK-PRE-LEN] Key size of preinstalled confidential cryptographic keys	33
88	5.1.12.6	[CRY-CCK-GEN] Default key size of generated confidential cryptographic keys	33
89	5.1.12.7	[CRY-PW-PRE-COM] Complexity of preinstalled passwords.....	33
90	5.1.12.8	[CRY-PW-GEN-COM] Default complexity of generated passwords	34
91	5.1.12.9	[CRY-PW-USR-COM] Recommended complexity of user chosen passwords	34
92	5.2	Requirements specifications for vulnerability handling activities related to the product	34
93	6	Assessing for compliance with requirements	34
94	6.1	Assessing for compliance with product's technical requirements specifications	34
95	6.1.1	General	34
96	6.1.2	Known exploitable vulnerabilities.....	34
97	6.1.2.1	Assessment criteria for [NKEV-SUM-SUPPORT]	34
98	6.1.2.2	Assessment criteria for [NKEV-SUM-PROVIDE]	36
99	6.1.2.3	Assessment criteria for [NKEV-SUM-AUTO]	37
100	6.1.2.4	Assessment criteria for [NKEV-SUM-NOTIF]	38
101	6.1.3	Default configuration	39
102	6.1.3.1	Assessment criteria for [SDC-AUM-FH]	39
103	6.1.3.2	Assessment criteria for [SDC-FRM]	40
104	6.1.4	Authentication and access control mechanisms	41
105	6.1.4.1	Assessment criteria for [ACM-FH]	41
106	6.1.4.2	Assessment criteria for [AUM-FH]	42
107	6.1.4.3	Assessment criteria for [AUTHZ-LP]	43
108	6.1.4.4	Assessment criteria for [AUTHZ-R]	44
109	6.1.5	Integrity protection.....	44
110	6.1.6	Confidentiality protection	44
111	6.1.7	Data minimization	44
112	6.1.7.1	Assessment criteria for [DMIN-DJST].....	44
113	6.1.8	Availability protection.....	45

114	6.1.8.1	Assessment criteria for [AVAI-TIME-RECO-POW].....	45
115	6.1.8.2	Assessment criteria for [AVAI-TIME-NETW].....	47
116	6.1.8.3	Assessment criteria for [AVAI-TIME-RECO-NETW].....	48
117	6.1.8.4	Assessment criteria for [AVAI-TIME-OUTA-NOT].....	50
118	6.1.8.5	Assessment criteria for [AVAI-TIME-PREV-NOT].....	51
119	6.1.8.6	Assessment criteria for [AVAI-TIME-NET-PRIO].....	52
120	6.1.8.7	Assessment criteria for [AVAI-TIME-RES-PRIO].....	53
121	6.1.8.8	Assessment criteria for [AVAI-TIME-IMP-AMP].....	54
122	6.1.8.9	Assessment criteria for [AVAI-TIME-DOS-RATE].....	55
123	6.1.8.10	Assessment criteria for [AVAI-SUM-SCHEDULE].....	56
124	6.1.9	Impact minimization	58
125	6.1.10	Limit attack surface.....	58
126	6.1.10.1	Assessment criteria for [LAS-SBOOT].....	58
127	6.1.11	Logging and monitoring mechanisms	59
128	6.1.11.1	Assessment criteria for [LOG-LOW].....	59
129	6.1.11.2	Assessment criteria for [LOG-MEDIUM].....	60
130	6.1.11.3	Assessment criteria for [LOG-HIGH].....	61
131	6.1.11.4	Assessment criteria for [LOG-TIME].....	62
132	6.1.11.5	Assessment criteria for [LOG-TIME-HIGH].....	63
133	6.1.11.6	Assessment criteria for [LOG-STORAGE].....	63
134	6.1.11.7	Assessment criteria for [LOG-BACKUP].....	64
135	6.1.12	Deletion mechanisms	65
136	6.1.12.1	Assessment criteria for [DLM-PERM].....	65
137	6.1.13	Other product's technical requirements specifications	67
138	6.1.13.1	Assessment criteria for [USERNOT-SECREL].....	67
139	6.1.13.2	Assessment criteria for [GUI-SECCONF].....	68
140	6.2	Assessment criteria for vulnerability handling activities related to the product	69
141	Annex A (informative):	Relationship between the present document and the requirements of	
142		EU Regulation 2024/2847.....	70
143	Annex B (informative):	Guidance for the application of the present document	76
144	Annex C (informative):	Information on the methodology for the assessment of cybersecurity	
145		risks used to develop the present document	80
146	C.1	Guidance for determining impact classes	80
147	C.1.1	General.....	80
148	C.1.2	confidential data.....	80
149	C.1.3	loss sensitive data.....	80
150	C.1.4	time sensitive data and time sensitive function	81
151	C.1.5	integrity relevant data and integrity relevant function.....	81
152	Annex D (normative):	Relationship between specific data and functions assets covered by	
153		the present document to impact classes for generic asset categories	83
154	D.1	Data assets	83
155	D.2	Function assets.....	85
156	Annex E (normative):	Protection measures.....	90
157	E.1	authentication mechanism strength.....	90
158	E.1.1	[AUM-FH] Authentication for functions whose use can cause harm	90
159	E.1.1.1	General	90
160	E.1.1.2	authentication - strength level basic	90
161	E.1.1.3	authentication - strength level normal	90
162	E.1.1.4	authentication - strength level enhanced.....	91
163	E.1.1.5	authentication - strength level strong.....	91
164	E.1.2	Assessment for authentication mechanism strength.....	91
165	E.1.2.1	Assessment criteria regarding the protection against limited presentation attacks.....	91
166	E.1.2.2	Assessment criteria regarding the protection against targeted presentation attacks	92
167	E.1.2.3	Assessment criteria regarding the protection against elaborate presentation attacks.....	92
168	E.1.2.4	Assessment criteria regarding the protection against limited brute force attacks.....	93
169	E.1.2.5	Assessment criteria regarding the protection against targeted brute force attacks.....	94

170	E.1.2.6	Assessment criteria regarding the protection against automated brute force attacks.....	94
171	E.1.2.7	Assessment criteria regarding the protection against presentation attacks	95
172	E.1.2.8	Assessment criteria regarding the protection against elaborate brute force attacks.....	96
173	E.1.2.9	Assessment criteria regarding the protection against automated security token spoofing attacks.....	96
174	E.1.2.10	Assessment criteria regarding the protection against targeted security token spoofing attacks.....	97
175	E.1.2.11	Assessment criteria regarding the protection against elaborate security token spoofing attacks.....	97
176	E.1.2.12	Assessment criteria regarding the protection against replay attacks.....	98
177	E.1.2.13	Assessment criteria regarding the protection against PitM attacks.....	99
178	E.2	integrity protection strength.....	100
179	E.2.1	[INT-SWPCK] Software package verification.....	100
180	E.2.1.1	General	100
181	E.2.1.2	software package integrity verification - strength level basic.....	100
182	E.2.1.3	software package integrity verification - strength level normal.....	100
183	E.2.1.4	software package integrity verification - strength level enhanced.....	100
184	E.2.2	[INT-COM] Communication of integrity relevant data	100
185	E.2.2.1	General	100
186	E.2.2.2	communication of integrity relevant data - protection strength level basic	100
187	E.2.2.3	communication of integrity relevant data - protection strength level normal	100
188	E.2.2.4	communication of integrity relevant data - protection strength level enhanced	101
189	E.2.2.5	communication of integrity relevant data - protection strength level strong	101
190	E.3	confidentiality protection strength	101
191	E.3.1	[CONF-SSM] Confidentiality protecting persistent storage for confidential data	101
192	E.3.1.1	General	101
193	E.3.1.2	confidential persistent storage - strength level basic	101
194	E.3.1.3	confidential persistent storage - strength level normal	101
195	E.3.1.4	confidential persistent storage - strength level enhanced.....	102
196	E.3.1.5	confidential persistent storage - strength level strong.....	102
197	E.3.2	[CONF-COM] Communication of confidential data.....	102
198	E.3.2.1	General	102
199	E.3.2.2	authentication - strength level strong.....	102
200	E.3.2.3	communication of confidential data - protection strength level normal	102
201	E.3.2.4	communication of confidential data - protection strength level enhanced.....	102
202	E.3.2.5	communication of confidential data - protection strength level strong.....	102
203	Annex F (informative):	Relationship between the present document and the covered/not	
204		covered cybersecurity risks.....	103
205	Annex G (informative):	Relationship between the present document and ETSI EN 303 645/	
206		ETSI TS 103 701	107
207			
208			

209 Intellectual Property Rights

210 Essential patents

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

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

220 Trademarks

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

225 **DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its
 226 Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the
 227 3GPP Organisational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of
 228 the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

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

230 Foreword

231 **DRAFT FOREWORD - DO NOT CONSIDER THE CONTENT**

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

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

240 Once the present document is cited in the Official Journal of the European Union under that Regulation, compliance
 241 with the normative clauses of the present document given in table A.1 confers, within the limits of the scope of the
 242 present document, a presumption of conformity with the corresponding requirements of that Regulation and associated
 243 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

244 Modal verbs terminology

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

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

249

250 1 Scope

251 The present document specifies vulnerability handling activities, technical requirements and corresponding assessment
 252 criteria for smart home products with security functionalities related to cybersecurity. The products with digital
 253 elements in scope, thereafter "smart home products with security functionalities":

- 254 • are specified within the "technical description" of the "category of product" number "17." by the Commission
 255 Implementing Regulation (EU) 2025/2392 [i.2] as:
 256 "Products with digital elements that protect the physical security of consumers in a residential setting and
 257 which can be controlled or managed remotely from other systems, as well as hardware and software that
 258 centrally control such products.
 259 This category includes but is not limited to smart door locking devices, baby monitoring systems, alarm
 260 systems and home security cameras." and
- 261 • are only covered within the product context described in clause 4.

262 The present document covers those products to demonstrate compliance with essential cybersecurity requirements in the
 263 Regulation (EU) 2024/2847 [i.1] under the conditions identified in annex A.

264 2 References

265 2.1 Normative references

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

269 Referenced documents which are not found to be publicly available in the expected location might be found in the [ETSI](#)
 270 [docbox](#).

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

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

274 [1] CEN/CLC JT013090:2026 (CEN/CLC prEN 40000-1-3): "Cybersecurity requirements for
 275 products with digital elements - Vulnerability Handling".

276 [2] [Agreed Cryptographic Mechanisms](#): "European Union Agency for Cybersecurity, European
 277 Cybersecurity Certification Group - Sub-group on Cryptography - Agreed Cryptographic
 278 Mechanisms".

279 2.2 Informative references

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

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

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

287 [i.1] [Regulation \(EU\) 2024/2847](#): "Regulation (EU) 2024/2847 of the European Parliament and of the
 288 Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital
 289 elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU)
 2020/1828 (Cyber Resilience Act)".

- 291 [i.2] [Regulation \(EU\) 2025/2392](#): "Commission Implementing Regulation (EU) 2025/2392 of 28
292 November 2025 on the technical description of the categories of important and critical products
293 with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of
294 the Council".
- 295 [i.3] [Standardisation request M/606 - C\(2025\)618](#): "Commission Implementing decision of 3.2.2025 on
296 a standardisation request to the European Committee for Standardisation (CEN), the European
297 Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications
298 Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU)
299 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal
300 cybersecurity requirements for products with digital elements and amending Regulations (EU) No
301 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)".
- 302 [i.4] CEN/CLC JT013095:2026 (CEN/CLC prEN 40000-1-1): "Cybersecurity requirements for
303 products with digital elements – Vocabulary".
- 304 [i.5] ETSI EN 304 623 vx.x.x: "Cyber Security (CYBER); CRA; Cybersecurity requirements for boot
305 managers".
- 306 [i.6] [ISO/IEC 24760-1:2025](#): "Information security, cybersecurity and privacy protection — A
307 framework for identity management - Part 1: Core concepts and terminology".

308 3 Definition of terms, symbols and abbreviations

309 3.1 Terms

310 For the purposes of the present document, the terms and definitions given in Regulation (EU) 2024/2847 [i.1],
311 CEN/CLC JT013095:2026 (CEN/CLC prEN 40000-1-1) [i.4] and the following apply:

312 ARCHITECTURE RELATED TERMS

313 **application software**: software designed to perform specific user- or SHPSF-oriented functional tasks on a device,
314 operating on top of the core software, and without direct responsibility for hardware initialization or fundamental
315 system control

316 EXAMPLE: a mobile app, desktop software or parts of architectural component's embedded software that
317 implements essential functionalities

318 NOTE: application software typically uses APIs provided by core software.

319 **architectural component**: self-contained hardware architectural component or software architectural component that is
320 part of the SHPSF

321 **core software**: any software that abstracts hardware, manages hardware resources and provides interfaces for other
322 software to interact with each other or the core software

323 EXAMPLE: a hardware architectural component's operating system, hardware abstraction layer or APIs for
324 application software

325 **hardware architectural component**: self-contained hardware part of the SHPSF including its associated software
326 architectural component

327 **software architectural component**: self-contained software part of the SHPSF

328 EXAMPLE: Companion-App, RDPS-Cloud-Application

329 ASSET CATEGORIES

330 **confidential data**: data asset, whose disclosure can have a negative impact

331 **data asset**: asset, that is data processed by the SHPSF

332 **function asset**: asset, that is a function of the SHPSF

333 **function, whose use can cause harm**: function asset that is:

- 334 • a function, whose use can impact the availability of other devices, services or networks,
- 335 • a function, whose use can impact the safety or privacy of human entities,
- 336 • a function, which can communicate confidential data,
- 337 • a function, which can communicate integrity relevant data,
- 338 • a function, which can modify integrity relevant data, or
- 339 • a function, which can modify integrity relevant functions

340 **integrity relevant data:** data asset, whose tampering can have a negative impact

341 **integrity relevant function:** function asset, whose tampering can have a negative impact

342 **loss sensitive data:** data asset, whose permanent loss has a negative impact

343 **time sensitive data:** data asset, where a time delay in availability has a negative impact

344 **time sensitive function:** function asset, where a time delay in availability has a negative impact

345 COMMUNICATION TYPES

346 **adjacent communication:** ingoing/outgoing communication from/to private networks which does not require physical
347 proximity to the communication partner

348 EXAMPLE: communication through a virtual-private-network tunnel with a communication partner in a private
349 network

350 **local communication:** ingoing/outgoing communication which requires physical proximity to but not physical presence
351 at the communication partner

352 EXAMPLE 1: point to point communication via short-range wireless technologies between two communication
353 partners.

354 EXAMPLE 2: radio communication between components of an alarm system or between alarm devices

355 **physical communication:** communication that requires physical interchange with the communication partner's
356 hardware or the hardware the communication partner runs on

357 EXAMPLE: direct communication with a chip after modification on a SHPSF's hardware architectural
358 component

359 **public communication:** ingoing/outgoing communication from/to public networks

360 EXAMPLE 1: communication via internet

361 EXAMPLE 2: alarm transmission through a public network

362 **strict local communication:** ingoing/outgoing communication which requires physical presence at the communication
363 partner

364 EXAMPLE 1: communication with a hardware architectural component via its key-pad

365 EXAMPLE 2: communication between a RF tag and tag reader of an alarm system

366 DATA ASSETS

367 **SHPSF state data:** data asset that contains SHPSF state information

368 **actuator control data:** data asset intended to control an actuator function

369 **audio input data:** data asset that represents audio information captured by the SHPSF

370 **authorization policy data:** data asset that contains an authorization policy

371 EXAMPLE: assignment of privileges to users

372 **battery status data:** data asset that represents the charge level of a device

373 **cryptographic security parameter:** data asset that determines the cryptographic operations of a cryptographic function

374 EXAMPLE: passwords, data hashes, message authentication codes, keys used for symmetric or asymmetric
 375 cryptography, (pseudo-)random numbers

376 **fire detection data:** data asset that indicates the presence of a fire

377 EXAMPLE: sensor data for physical parameters related to a fire such as temperature distributions or
 378 photoelectrical signals (detecting smoke)

379 **function configuration data:** data asset intended to configure a function asset

380 **function fault detection data:** data asset that indicates a detected fault of a function provided by a device or system

381 **human fall detection data:** data asset that indicates whether a human fell and might need help

382 **inflammable/explosive gas detection data:** data asset that indicates the presence of an inflammable or explosive gas

383 EXAMPLE: sensor data for physical parameter related to inflammable or explosive gases such as infrared
 384 absorption

385 **intrusion detection data:** data asset that indicates the presence of a being in supervised premises

386 **locking element position data:** data asset that represents the physical position or state of the locking element of a lock

387 EXAMPLE: data representing the position of bolt, latch or related to a comparable mechanism

388 **logging data:** data asset that contains information logged by logging mechanisms

389 **network status data:** data asset that describes an architectural component's network connections status

390 **object tamper detection data:** data asset that indicates whether an object is tampered

391 **software package:** data asset that contains software intended to be installed on the SHPSF

392 **video input data:** data asset that represents video information captured by the SHPSF

393 EXAMPLE: video or picture recordings processed (including storage) on the SHPSF

394 **window/door opening status data:** data asset that indicates whether a window or door has been opened

395 DATA RELATED TERMS

396 **confidential cryptographic key:** confidential data that is not an initialisation vector or password which is used in the
 397 operation of a cryptographic function

398 EXAMPLE: symmetric keys, private keys

399 NOTE: A confidential cryptographic key is a cryptographic security parameter

400 **data:** information in digital form

401 **location data:** data containing geographical information

402 **password:** sequence of characters used to authenticate an entity that is intended to be used by humans as an
 403 authentication factor of type knowledge

404 EXAMPLE: symmetric keys, private keys

405 NOTE 1: "A password is a cryptographic security parameter"

406 NOTE 2: "passwords are sometimes chosen to be remembered by humans such as 4-digit PINs"

407 NOTE 3: "passwords are sometimes chosen to be complex e.g. when generated by a password manager under a
 408 respective configuration"

409 **processed data:** data processed by the SHPSF, including but not limited to capturing, storing, transmitting, modifying,
 410 deleting and presenting data

411 **public data:** data from publicly accessible sources

412 **user-related data:** data provided by a user and/or about a user

413 FUNCTION ASSETS

- 414 **SHPSF actuator alarm function:** SHPSF actuator function that alarms in hazardous situations
- 415 EXAMPLE: Functionality of emitting loud sound or bright lightning signals to attract e.g. neighbourhoods' or
416 household members' attention to a potential fire or an unauthorized physical access to a protected
417 area.
- 418 NOTE: As defined a SHPSF actuator alarm function does not include a function to communicate alarm data via a
419 logical interface. However, such a function falls under SHPSF function which can communicate alarm
420 data.
- 421 **SHPSF basic protection object lock function:** SHPSF actuator function that can change the securement state of a
422 locking mechanism that is intended to control access to low value objects outside or inside a residence.
- 423 NOTE: Such functions can include opening/closing a simple padlock
- 424 **SHPSF exterior lock function:** SHPSF actuator function that can change the securement state of a locking mechanism
425 that is intended to control access from outside a residence to the inside.
- 426 NOTE: Such functions can include opening/closing the door of a resident's house or apartment.
- 427 **SHPSF high protection object lock function:** SHPSF actuator function that can change the securement state of a
428 locking mechanism that is intended to control access to high value objects outside or inside a residence.
- 429 NOTE: Such functions can include opening/closing a vault
- 430 **SHPSF interior lock function:** SHPSF actuator function that can change the securement state of a locking mechanism
431 that is intended to control access within a residence.
- 432 NOTE: Such functions can include opening/closing the door within a resident's house or apartment.
- 433 **SHPSF lock function with failsafe:** SHPSF actuator function, that locks or unlocks a lock, with a physical failsafe
- 434 **SHPSF medium protection object lock function:** SHPSF actuator function that can change the securement state of a
435 locking mechanism that is intended to control access to medium value objects outside or inside a residence.
- 436 NOTE: Such functions can include opening/closing a physical protected mailbox lock or garden cabin lock
- 437 **SHPSF physical tamper detection function:** SHPSF function to detect physical tampering of a hardware architectural
438 component
- 439 **SHPSF surrounding monitoring function:** SHPSF function that monitors noise level or movement
- 440 **access control mechanism:** SHPSF function that enforces an authorization policy
- 441 **actuator control function:** function asset intended to control an actuator function
- 442 **audio input function:** SHPSF function that converts audio signals into data
- 443 **audio output function:** SHPSF function that converts data into audio signals
- 444 **authentication mechanism:** SHPSF function that verifies an entity's claimed identity
- 445 **bootloader function:** SHPSF function that initiates the execution of other core software at start up.
- 446 **configuration function:** SHPSF function that allows to change the configuration of SHPSF's functions
- 447 **connection function:** SHPSF function that is used for testing or establishing communication capability via machine
448 interface
- 449 EXAMPLE: ICMP, DHCP Discovery, function of a SHPSF establishing the connection for remote access or
450 remote alarm transmission
- 451 NOTE: In this context, establishing communication means communication without user-related data and without
452 authentication of the communication partner for the purpose of establishment of a connection.
- 453 **cryptographic function:** SHPSF function that performs cryptographic algorithm

- 454 **data backup mechanism:** SHPSF function that copies data assets to persistent storage of another architectural
 455 component or target outside the SHPSF.
- 456 **data presenting function:** SHPSF function that grants an entity read access to data or presents data to a user via
 457 physical human interface
- 458 EXAMPLE 1: Presenting data to a user on a website associated with a RDPS
 459 EXAMPLE 2: Presenting data on a display, controlling indicator lights
- 460 **detection function:** SHPSF function that detects a certain event
- 461 EXAMPLE: A function that monitors the data from a temperature sensor and detects when a certain threshold
 462 temperature is exceeded.
- 463 NOTE: When the event is a hazardous situation it is (also) a physical security detection function.
- 464 **factory reset function:** SHPSF function that removes all user-related data and sets the architectural components in a
 465 factory default state, potentially keeping software updates
- 466 **fire/gas alarm function :** SHPSF actuator function that alarms the presence of a fire or inflammable/explosive gas
 467 hazard in supervised premises
- 468 **input sanitization mechanism:** SHPSF function that scans function input data based on a function specific pattern and
 469 removes or alters parts, that can lead to incidents
- 470 EXAMPLE: If external data input is amongst others intended to be stored via a database service, escape
 471 characters and other database service specific commands (defined by a corresponding function
 472 specific pattern) are removed from the external data input, before it is processed by the database
 473 service.
- 474 **input validation mechanism:** SHPSF function that rejects input data if it does not meet an accepted pattern
- 475 EXAMPLE: The input is expected to be the users' year of birth. Data type validation is used to ensure the input
 476 to be an integer followed by a range validation checking that the input is between 1900 and the
 477 current year.
- 478 **intrusion and hold up alarm function :** SHPSF actuator function that alarms
- 479 • at presence, entry or attempted entry of an intruder into supervised premises and/or
 480 • when a user deliberately generates a hold-up alarm condition
- 481 **logging mechanism:** SHPSF function that logs events
- 482 **monitoring mechanism:** SHPSF function that frequently measures functional metrics of the SHPSF
- 483 **notification mechanism:** SHPSF function that notifies entities on certain events
- 484 **object tamper detection function:** SHPSF function that detects tampering of an object
- 485 **physical security detection function:** SHPSF function that detects a hazardous situation
- 486 EXAMPLE: The detection function of an alarm system or an alarm device.
- 487 **physical security notification function:** SHPSF actuator function that notifies users in hazardous situations
- 488 EXAMPLE: Function that controls the sounder of a smoke alarm device.
- 489 **positioning function:** SHPSF function that estimates or derives the architectural component's position based on
 490 available inputs.
- 491 **power supply function:** SHPSF actuator function that supplies power to hardware architectural components
- 492 EXAMPLE: The power supply equipment that supplies power to components of an alarm system
- 493 **real-time service or clock:** service or function that provides real time information
- 494 **sensing function:** SHPSF function to measure characteristics of its physical operational environment
- 495 **social alarm function :** SHPSF actuator function that alarms when the user may need urgent help

496 **software package verification mechanism:** SHPSF function that verifies the integrity and authenticity of software
497 packages

498 **software update mechanism:** SHPSF function that receives and installs software updates

499 **time service or function:** service or function that provides time information

500 **video input function:** SHPSF function that converts video signals into data

501 **video output function:** SHPSF function that converts data into video signals

502 **FUNCTION RELATED TERMS**

503 **actuator function:** function that performs an action on the physical operational environment

504 **authorization policy:** policy that describes the access rights of entities on SHPSF's data and functions

505 **automated update:** a software update that does not require an explicit trigger by a user

506 **EXAMPLE 1:** An update is automatically downloaded from the internet, verified and installed without user
507 interaction when an internet connection is available.

508 **EXAMPLE 2:** A hardware architectural component with only local communication capabilities receives the
509 update from another architectural component in its proximity. The other architectural component
510 has a connection to the internet and downloads the software for the hardware architectural
511 component without user interaction. The hardware architectural component is can only be
512 automatically updated when the other architectural component is in its proximity.

513 **cryptographic algorithm:** sequence of instructions based on mathematical properties to protect confidentiality,
514 integrity or authenticity against attackers.

515 **NOTE:** Cryptographic algorithms include cryptographic protocols/schemes/constructors/primes such as TLS/
516 Symmetric Entity Authentication Schemes/AES-128 as part of a CMAC/AES-256

517 **function output:** output of an architectural component's functions that is:

- 518 • a modification or creation of SHPSFs' data or functions
- 519 • information intended to inform human users
- 520 • information intended to inform or control devices or services, or
- 521 • an action on the physical operational environment

522 **NOTE:** function output that is an action on the physical operational environment can be performed by a SHPSF's
523 actuator function.

524 **function trigger input:** input to an architectural component's functions provided by:

- 525 • human users,
- 526 • devices or services, or
- 527 • the physical operational environment

528 **NOTE:** function trigger input provided by the physical operational environment can be received by a SHPSF's
529 sensing function.

530 **identity:** set of attributes related to an entity

531 **NOTE:** SOURCE: ISO/IEC 24760-1:2025 [i.6]

532 **residential physical security function:** function which provides function output as reaction to function trigger input
533 related to residential physical security

534 **INTERFACES**

535 **human interface:** interface that is intended to be used by human

- 536 EXAMPLE: PIN pad, touch screen, web interface for user login and user product management
 537 **interface:** shared boundary across which the SHPSF exchanges information
- 538 **logical human interface:** interface that is a human interface and a logical interface
- 539 EXAMPLE: web page for remote access
 540 NOTE: An external client used for remote access providing a logical human interface typically uses a machine
 541 interface to communicate with the SHPSF
- 542 **logical interface:** interface that does not exist in hardware and can only be used by using another device or a physical
 543 interface of a SHPSF
- 544 **machine interface:** interface that is intended to be used for machine-to-machine communication
- 545 EXAMPLE: Interfaces for USB/Bluetooth®/Ethernet/Wi-Fi®/DECT/DECT-2020 NR or debug ports
 546 accessible from outside the SHPSF
 547 **physical human interface:** interface that is a human interface and a physical interface
- 548 EXAMPLE: keypad, display, biometric reader, microphone, loudspeaker, (video) camera, touchscreen
 549 **physical interface:** interface that is part of the hardware of a SHPSF
- 550 EXAMPLE: USB/RJ45/JTAG ports, microSD/SIM card slot
 551 **OPERATIONAL ENVIRONMENTS**
- 552 **confined operational environment:** physical operational environment, where the geographical location is confined to a
 553 specific area
- 554 **fully controlled physical operational environment:** physical operational environment, where physical access is fully
 555 controlled by the user or trusted persons
- 556 EXAMPLE: private house or apartment
 557 **logical operational environment:** operational environment describing the accessibility via logical interfaces
- 558 **mobile operational environment:** physical operational environment, where the geographical location is changing
 559 during operation and not confined to a specific area
- 560 NOTE: Physical operational environment of smartphones and wearables
- 561 **operational environment:** System used to model to likelihood of incidents depending on the physical operational
 562 environment of the SHPSF, or parts of it, and the logical operational environment of the relevant logical interfaces.
- 563 **partially controlled physical operational environment:** physical operational environment, that is not a fully
 564 controlled physical operational environment and either under the control of a limited set of persons or located in an area
 565 where untrusted physical access is suspicious
- 566 EXAMPLE: Shared area in a house with different apartments or private property where public access is not
 567 intended.
 568 **physical operational environment:** operational environment determining the physical accessibility of an architectural
 569 component
- 570 **stationary operational environment:** physical operational environment, where the geographical location is fixed
- 571 **uncontrolled physical operational environment:** physical operational environment, where physical access control on
 572 arbitrary untrusted entities cannot be ensured for prolonged time periods and where untrusted physical access is not
 573 necessarily suspicious
- 574 EXAMPLE: Areas intended for public access
 575 **USERS**
- 576 **user:** natural entity that directly interacts with the SHPSF
- 577 NOTE: This includes all natural entities that interact directly with the SHPSF as the final product, but not
 578 manufactures for integration in other products.

579 3.2 Abbreviations

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

581 GENERAL

582	DHCP	Dynamic Host Configuration Protocol
583	GPS	Global Positioning System
584	GUI	Graphical User Interface
585	ICMP	Internet Control Message Protocol
586	PSF	Residential Physical Security Function
587	RDPS	Remote Data Processing Solution
588	USB	Universal Serial Bus
589	SHPSF	Smart Home Product With Security Functionalities

590 COMMUNICATION TYPES

591	COM	communication type
592	COM.Adjacent	adjacent communication
593	COM.Any	unspecified communication type
594	COM.Local	local communication
595	COM.Physical	physical communication
596	COM.Public	public communication
597	COM.StrictLocal	strict local communication

598 IMPACT CLASSES

599	IMP	impact class
600	IMP.AVAI.LOSS	loss sensitive availability impact class
601	IMP.AVAI.LOSS.High	loss sensitive availability impact class high
602	IMP.AVAI.LOSS.Low	loss sensitive availability impact class low
603	IMP.AVAI.LOSS.Medium	loss sensitive availability impact class medium
604	IMP.AVAI.TIME	time sensitive availability impact class
605	IMP.AVAI.TIME.High	time sensitive availability impact class high
606	IMP.AVAI.TIME.Low	time sensitive availability impact class low
607	IMP.AVAI.TIME.Medium	time sensitive availability impact class medium
608	IMP.CONF	confidentiality impact class
609	IMP.CONF.High	confidentiality impact class high
610	IMP.CONF.Low	confidentiality impact class low
611	IMP.CONF.Medium	confidentiality impact class medium
612	IMP.FH	impact class for function, whose use can cause harm
613	IMP.FH.CCON	function, which can communicate confidential data impact class
614	IMP.FH.CCON.High	function, which can communicate confidential data impact class high
615	IMP.FH.CCON.Low	function, which can communicate confidential data impact class low
616	IMP.FH.CCON.Medium	function, which can communicate confidential data impact class medium
617	IMP.FH.DSN	function, whose use can impact the availability of other devices, services or networks impact class
618	IMP.FH.DSN.High	function, whose use can impact the availability of other devices, services or networks impact class high
619	IMP.FH.DSN.Low	function, whose use can impact the availability of other devices, services or networks impact class low
620	IMP.FH.DSN.Medium	function, whose use can impact the availability of other devices, services or networks impact class medium
621	IMP.FH.High	function, whose use can cause harm impact class high
622	IMP.FH.Low	function, whose use can cause harm impact class low
623	IMP.FH.MINT	function, which can modify integrity relevant data impact class
624	IMP.FH.MINT.High	function, which can modify integrity relevant data impact class high
625	IMP.FH.MINT.Low	function, which can modify integrity relevant data impact class low
626	IMP.FH.MINT.Medium	function, which can modify integrity relevant data impact class medium
627	IMP.FH.Medium	function, whose use can cause harm impact class medium
628	IMP.FH.SP	function, whose use can impact the safety or privacy of human entities impact class
629	IMP.FH.SP.High	function, whose use can impact the safety or privacy of human entities impact class high
630	IMP.FH.SP.Low	function, whose use can impact the safety or privacy of human entities impact class low
631	IMP.FH.SP.Medium	function, whose use can impact the safety or privacy of human entities impact class medium

635	IMP.High	impact class high
636	IMP.INT	integrity impact class
637	IMP.INT.High	integrity impact class high
638	IMP.INT.Low	integrity impact class low
639	IMP.INT.Medium	integrity impact class medium
640	IMP.Low	impact class low
641	IMP.Medium	impact class medium

642 INTERFACES

643	IF	interface
644	IF.Any	unspecified interface
645	IF.Human	human interface
646	IF.HumanLogical	logical human interface
647	IF.HumanPhysical	physical human interface
648	IF.Logical	logical interface
649	IF.Machine	machine interface
650	IF.Physical	physical interface

651 OPERATIONAL ENVIRONMENTS

652	POE	physical operational environment
653	POE.Any	unspecified physical operational environment
654	POE.Confined	confined operational environment
655	POE.FullyControlled	fully controlled physical operational environment
656	POE.Mobile	mobile operational environment
657	POE.PartiallyControlled	partially controlled physical operational environment
658	POE.Stationary	stationary operational environment
659	POE.Uncontrolled	uncontrolled physical operational environment

660 PROTECTION MEASURE STRENGTH LEVEL

661	AUTH.Basic	authentication - strength level basic
662	AUTH.Enhanced	authentication - strength level enhanced
663	AUTH.Normal	authentication - strength level normal
664	AUTH.Strong	authentication - strength level strong
665	CONF.COM.Basic	communication of confidential data - protection strength level strong
666	CONF.COM.Enhanced	communication of confidential data - protection strength level enhanced
667	CONF.COM.Normal	communication of confidential data - protection strength level normal
668	CONF.COM.Strong	communication of confidential data - protection strength level strong
669	CONF.SSM.Basic	confidential persistent storage - strength level basic
670	CONF.SSM.Enhanced	confidential persistent storage - strength level enhanced
671	CONF.SSM.Normal	confidential persistent storage - strength level normal
672	CONF.SSM.Strong	confidential persistent storage - strength level strong
673	INT.COM.Basic	communication of integrity relevant data - protection strength level basic
674	INT.COM.Enhanced	communication of integrity relevant data - protection strength level enhanced
675	INT.COM.Normal	communication of integrity relevant data - protection strength level normal
676	INT.COM.Strong	communication of integrity relevant data - protection strength level strong
677	INT.SW.VER.Basic	software package integrity verification - strength level basic
678	INT.SW.VER.Enhanced	software package integrity verification - strength level enhanced
679	INT.SW.VER.Normal	software package integrity verification - strength level normal
680	INT.SW.VER.Strong	software package integrity verification - strength level strong
681	N/A	not applicable

682 4 Product context

683 4.1 Product functions

684 4.1.1 Residential physical security function

685 The present document addresses the following essential functionalities of SHPSF:

- 686 • PSFs that might make use of the following functions:

- 687 - audio input function
- 688 - video input function
- 689 - audio output function
- 690 - video output function
- 691 - SHPSF exterior lock function
- 692 - SHPSF interior lock function
- 693 - SHPSF basic protection object lock function
- 694 - SHPSF medium protection object lock function
- 695 - SHPSF high protection object lock function
- 696 - SHPSF actuator alarm function
- 697 - SHPSF actuator control function
- 698 - SHPSF function which can communicate SHPSF data
- 699 - SHPSF function which can modify SHPSF data

700 4.1.2 Supporting functions

701 The present document addresses the following supporting functionalities of SHPSF:

- 702 • configuration function
- 703 • software update mechanism
- 704 • monitoring mechanism
- 705 • notification mechanism
- 706 • logging mechanism
- 707 • access control mechanism
- 708 • authentication mechanism
- 709 • factory reset function
- 710 • integrity protecting communication mechanism
- 711 • confidentiality protecting communication mechanism
- 712 • integrity protecting secure storage mechanism
- 713 • confidentiality protecting secure storage mechanism
- 714 • deletion mechanism
- 715 • onboarding mechanism
- 716 • input sanitization mechanism
- 717 • input validation mechanism
- 718 • software package verification mechanism
- 719 • bootloader function

- 720 • time service or function
- 721 • real-time service or clock
- 722 • cryptographic function
- 723 • data backup mechanism

724 4.1.3 Data assets

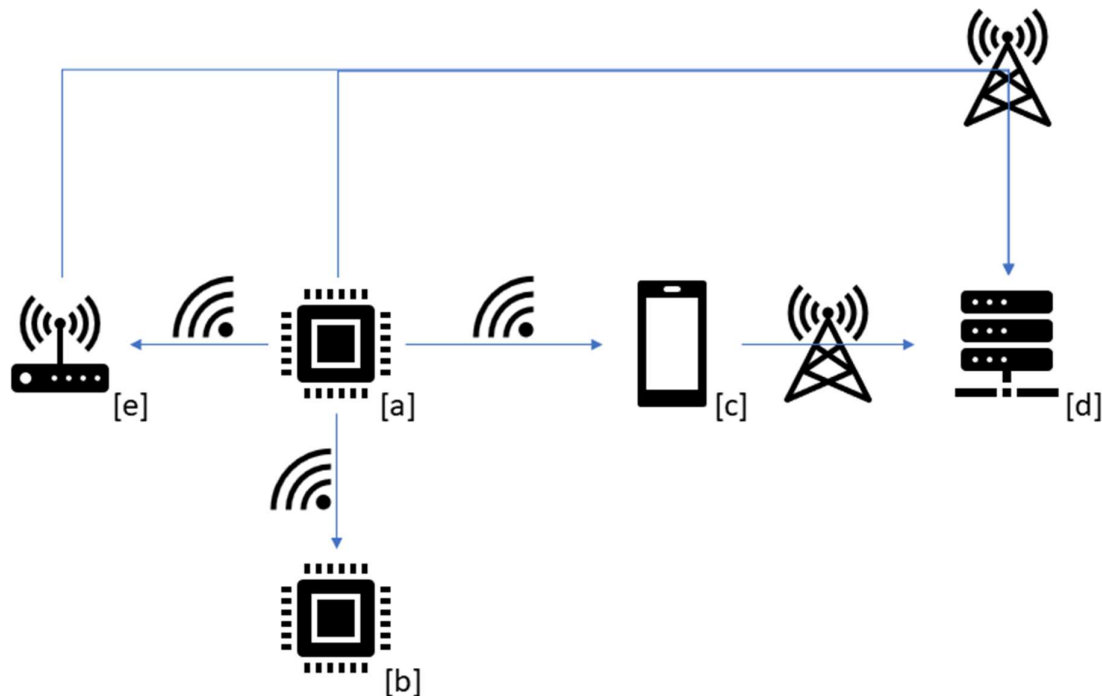
725 The essential and supporting functionalities might process the following data assets:

- 726 • SHPSF state data
- 727 • actuator control data
- 728 • audio input data
- 729 • authorization policy data
- 730 • battery status data
- 731 • cryptographic security parameter
- 732 • fire detection data
- 733 • function configuration data
- 734 • function fault detection data
- 735 • human fall detection data
- 736 • inflammable/explosive gas detection data
- 737 • intrusion detection data
- 738 • locking element position data
- 739 • logging data
- 740 • network status data
- 741 • object tamper detection data
- 742 • software package
- 743 • video input data
- 744 • window/door opening status data

745 4.2 Product Architecture

746 The architecture of a SHPSF consists of hardware architectural components and/or software architectural components.

747 NOTE: It is possible that a SHPSF consists of only one hardware architectural component.



748

749

Figure 1: Architectural Components and possible connections between them

750

Exemplary architectural components and possible connections between them are shown in figure 1. The following components are shown in the figure:

751

752

(a) SHPSF's hardware architectural component

753

(b) Another product's hardware architectural component

754

(c) SHPSF's mobile application (software architectural component) installed on a smartphone

755

(d) SHPSF's cloud RDPS (software architectural component) installed on a server

756

(e) SHPSF's gateway (hardware architectural component)

757

NOTE: Not all subsets of the SHPSF's architectural components in this example are necessary for falling into the scope of the present document.

758

759

4.3 Operational Environment

760

The present document addresses the following operational environments of SHPSF.

761

For the logical operational environment, the following digital communication types are addressed for any architectural component of the SHPSF:

762

763

- **public communication** - COM.Public,

764

- **adjacent communication** - COM.Adjacent,

765

- **local communication** - COM.Local,

766

- **strict local communication** - COM.StrictLocal.

767

The following physical operational environments are addressed for any hardware architectural component of the SHPSF:

768

- 769 • **fully controlled physical operational environment** - POE.FullyControlled,
- 770 • **partially controlled physical operational environment** - POE.PartiallyControlled,
- 771 • **mobile operational environment** - POE.Mobile.

772 The following physical operational environments are addressed for any software architectural component's host device
773 where it is intended or reasonably foreseen to be installed:

- 774 • **fully controlled physical operational environment** - POE.FullyControlled,
- 775 • **partially controlled physical operational environment** - POE.PartiallyControlled,
- 776 • **mobile operational environment** - POE.Mobile.

777 4.4 Interfaces

778 The present document addresses the following interfaces of the SHPSF:

- 779 • **human interface** - IF.Human
- 780 • **machine interface** - IF.Machine
- 781 • **logical interface** - IF.Logical
- 782 • **physical interface** - IF.Physical

783 4.5 Distribution of security functions

784 The present document addresses the distribution of security functions among the SHPSF and other products with digital
785 elements in the SHPSF's context (e.g. host devices for SHPSF's software architectural components) by the following
786 expressions used to formulate the technical requirements specifications in clause [5.1](#).

787 "The SHPSF shall [...] use [some expression related to security functions]" means:

- 788 • the SHPSF itself provides those security functions which are always used, or
- 789 • other products with digital elements in the SHPSF's context provide those security functions which are always
790 used by the SHPSF.

791 "The SHPSF shall [...] support [some expression related to security functions]" means:

- 792 • the SHPSF itself provides those security functions, or
- 793 • other products with digital elements in the SHPSF's context provide those security functions.

794 "The SHPSF shall [...] provide [some expression related to security functions]" means that the SHPSF itself provides
795 those security functions.

796 Situations where the SHPSF itself does not provide security functions that are required to be used or supported by the
797 SHPSF and other products with digital elements in the SHPSF's context do not provide those security functions, are
798 addressed in the requirement [USERNOT-NOSECFUC] in clause [5.1.12](#).

799 4.6 Users

800 The present document addresses the following using entities of SHPSF:

- 801 • Consumers for private usage
- 802 • Service providers for professional installation, commissioning and/or maintenance
- 803 • Manufactures for integration in other products with digital elements intended for consumers

804 4.7 Use cases

805 4.7.1 General

806 The present document addresses all use cases that can be constructed by the previous elements of clause [4](#).

807 4.7.2 Use case profiles

808 In order to classify use cases and to define security profiles the following use case profiles are defined. Those
809 definitions make use of impact classes of functions. The functions covered by the present document are provided in
810 clause [4.1](#), their impact classes in annex [D](#).

811 Use case profile for low impact functions

812 The use case profile for low impact functions bundles all use cases addressed by the present document where the
813 maximum impact identified for (IMP.FH, IMP.AVAI.TIME) of a SHPSF's function falls under IMP.Low.

814 Use case profile for medium impact functions

815 The use case profile for medium impact functions bundles all use cases addressed by the present document where the
816 maximum impact identified for (IMP.FH, IMP.AVAI.TIME) of a SHPSF's function falls under IMP.Medium.

817 Use case profile for high impact functions

818 The use case profile for high impact functions bundles all use cases addressed by the present document where the
819 maximum impact identified for (IMP.FH, IMP.AVAI.TIME) of a SHPSF's function falls under IMP.High.

820 4.8 Security Profiles

821 Based on the use case profiles defined in clause [4.7.2](#) the following security profiles with assigned requirements in
822 table [1](#) are defined:

- 823 • security profile for low impact functions
- 824 • security profile for medium impact functions
- 825 • security profile for high impact functions

826

Table 1: Security profiles with corresponding requirements

Requirement	Security profile for		
	Low impact functions	Medium impact functions	High impact functions
[NKEV-MKAV]	X	X	X
[NKEV-SUM-SUPPORT]	X	X	X
[NKEV-SUM-PROVIDE]	X	X	X
[NKEV-SUM-AUTO]	X	X	X
[NKEV-SUM-NOTIF]	X	X	X
[SDC-AUM-FH]	X	X	X
[SDC-SUM-AUTO]	X	X	X
[SDC-SUM-NOTIF]	X	X	X
[SDC-FRM]	X	X	X
[ACM-FH]	X	X	X
[AUM-FH]	X	X	X
[AUTHZ-LP]	X	X	X
[AUTHZ-R]	X	X	X
[INT-SWPCK]	X	X	X
[INT-COM]	X	X	X
[CONF-SSM]	X	X	X
[CONF-COM]	X	X	X
[AVAI-TIME-RECO-POW]	X	X	X
[AVAI-TIME-NETW]	X	X	X
[AVAI-TIME-RECO-NETW]	X	X	X
[AVAI-TIME-OUTA-NOT]		X	X
[AVAI-TIME-PREV-NOT]			X
[AVAI-TIME-NET-PRIO]		X	X
[AVAI-TIME-RES-PRIO]		X	X
[AVAI-TIME-IMP-AMP]		X	X
[AVAI-TIME-DOS-RATE]			X
[AVAI-SUM-SCHEDULE]		X	X
[LAS-INVAL]	X	X	X
[LAS-INSAN]	X	X	X
[LAS-PHY-INF]	X	X	X
[LAS-LOGIC-INF]	X	X	X
[LAS-APP]	X	X	X
[LAS-SBOOT]			X
[DMIN-DJST]	X	X	X
[LOG-LOW]	X		
[LOG-MEDIUM]		X	
[LOG-HIGH]			X
[LOG-TIME]	X	X	
[LOG-TIME-HIGH]			X
[LOG-STORAGE]		X	X
[LOG-BACKUP]			X
[USERNOT-NOSECFUC]	X	X	X
[USERNOT-SECREL]	X	X	X
[GUI-SECCONF]	X	X	X
[CRY-SOTA]	X	X	X
[CRY-CCK-PRE-LEN]	X	X	X
[CRY-CCK-GEN]	X	X	X
[CRY-PW-PRE-COM]	X	X	X
[CRY-PW-GEN-COM]	X	X	X
[CRY-PW-USR-COM]	X	X	X

827

5 Requirements specifications

828

5.1 Product's technical requirements specifications

829

5.1.1 Known exploitable vulnerabilities

830 5.1.1.1 [NKEV-MKAV] No known exploitable vulnerabilities

831 In accordance with the vulnerability handling specified in CEN/CLC JT013090:2026 (CEN/CLC prEN 40000-1-3) [1],
832 the SHPSF shall prior to making available on the market have no insufficiently mitigated known exploitable
833 vulnerabilities.

834 NOTE 1: The known exploitable vulnerabilities that occur after making the SHPSF available on the market are
835 subject to the vulnerability handling in CEN/CLC JT013090:2026 (CEN/CLC prEN 40000-1-3) [1].

836 NOTE 2: Typically, products are supplied with all necessary security updates during the first start up and after the
837 products have connection to a network over which security updates can be delivered.

838 5.1.1.2 [NKEV-SUM-SUPPORT] Secure software update mechanism

839 The SHPSF shall support software update mechanisms, that allow to update every part of the SHPSF's software, except
840 for parts of the SHPSF's software, that are immutable due to technical reasons.

841 EXAMPLE: An application distribution platform installed on a mobile device provides updates for mobile
842 applications. In some cases, where the application to be updated is part of the wearable's core
843 software, the core software update mechanism provides also the application updates.

844 NOTE: Part of the wearable's software can be immutable due to its technology (e.g. software installed in a ROM)

845 5.1.1.3 [NKEV-SUM-PROVIDE] Secure software update mechanism for core 846 components

847 All architectural components of the SHPSF that include core software shall provide software update mechanisms, that
848 allow to update every part of the architectural components software, except for parts of the architectural components
849 software, that are immutable due to security.

850 NOTE: A mobile application typically does not need to provide an update mechanism

851 5.1.1.4 [NKEV-SUM-AUTO] Automated security updates

852 Where the SHPSF has the capability to connect to a public network, the SHPSF shall support the automated update of
853 its software.

854 5.1.1.5 [NKEV-SUM-NOTIF] Update notifications

855 Where the SHPSF has the capability to connect to a public network, the SHPSF shall support the automated notification
856 of its users, when updates of its software are available.

857 5.1.2 Default configuration

858 5.1.2.1 [SDC-AUM-FH] Default configuration of authentication for functions whose 859 use can cause harm

860 The SHPSF shall by default be configured to use authentication mechanisms that meet

- 861 • the authentication mechanisms strengths specified in clause [E.1.1](#) and
- 862 • the minimal authentication mechanisms' strength determined by table [3](#),

863 except for connection functions.

864 NOTE: The support of authentication for functions whose use can cause harm is addressed in [AUM-FH].

865 5.1.2.2 [SDC-SUM-AUTO] Default configuration of automated security updates

866 Where

- 867 • the SHPSF has the capability to connect to a public network; and
- 868 • no time sensitive function with IMP.AVAI.TIME.High is provided by an architectural component,

869 the architectural component shall by default be configured to use automated software update mechanisms for its
870 software.

871 NOTE 1: The support of automated security updates is addressed in [NKEV-SUM-AUTO].

872 NOTE 2: The user can decide to turn off the automated security update mechanism and manually perform the
873 update when is more suitable for him.

874 5.1.2.3 [SDC-SUM-NOTIF] Default configuration of update notifications

875 The SHPSF shall by default be configured to use automated notification of its users, when updates of the SHPSF's
876 software are available.

877 NOTE: The support of update notification is addressed in [NKEV-SUM-NOTIF].

878 5.1.2.4 [SDC-FRM] Factory reset to restore the default state

879 The SHPSF shall provide a factory reset mechanism that allows a user to restore the default state, including the deletion
880 of all user-related data, installed applications, and configurations deviating from the default state.

881 NOTE 1: It is also possible that the factory reset will delete the installed security updates if these are installed
882 automatically or on request when the device is commissioned again.

883 NOTE 2: ANNEX II 8. d) of Regulation (EU) 2024/2847 [i.1] contains legal obligations on how users of the
884 SHPSF are informed about secure decommissioning of the SHPSF.

885 5.1.3 Authentication and access control mechanisms

886 5.1.3.1 [ACM-FH] Access control for functions whose use can cause harm

887 The SHPSF shall use access control mechanisms to control entities' use of functions whose use can cause harm, where
888 the applicability of this requirement is determined by table 2 except for connection functions.

889 **Table 2: Assignment for access control mechanisms**

			Impact class for function, whose use can cause harm		
			IMP.FH.Low	IMP.FH.Medium	IMP.FH.High
Attack Surface determined by COM, IF and POE of the architectural component that receives function trigger input	COM.StrictLocal via IF.Any	POE.FullyControlled	N/A	N/A	applicable[*]
		POE.PartiallyControlled	N/A	applicable	applicable
		POE.Mobile	applicable	applicable	applicable
	COM.Local via IF.HumanPhysical	POE.FullyControlled	N/A	applicable	applicable
		POE.PartiallyControlled	applicable	applicable	applicable
		POE.Mobile	applicable	applicable	applicable
	COM.Local via a non-IF.HumanPhysical	POE.Any	applicable	applicable	applicable
	COM.Adjacent via IF.Any		applicable	applicable	applicable
	COM.Public via IF.Any		applicable	applicable	applicable

890 For protection measures that are labelled with [*] it is not required that the SHPSF uses access control mechanisms for
891 its following functions:

- 892 • factory reset function

893 5.1.3.2 [AUM-FH] Authentication for functions whose use can cause harm

894 The SHPSF shall support authentication mechanisms, to authenticate entities using functions whose use can cause harm
895 before generating function output, where

- 896 • the authentication mechanisms strengths' are specified in clause [E.1.1](#) and
- 897 • the minimal required authentication strength is determined by table [3](#),
- 898 except for connection functions.

899

Table 3: Assignment for authentication mechanisms strengths

			Impact class for function, whose use can cause harm		
			IMP.FH.Low	IMP.FH.Medium	IMP.FH.High
Attack Surface determined by COM, IF and POE of the architectural component that receives function trigger input	COM.StrictLocal via IF.Any	POE.FullyControlled	N/A	N/A	AUTH.Normal[*]
		POE.PartiallyControlled	N/A	AUTH.Basic	AUTH.Normal
		POE.Mobile	AUTH.Basic	AUTH.Normal	AUTH.Enhanced
	COM.Local via IF.HumanPhysical	POE.FullyControlled	N/A	AUTH.Basic	AUTH.Normal
		POE.PartiallyControlled	AUTH.Basic	AUTH.Normal	AUTH.Enhanced
		POE.Mobile	AUTH.Basic	AUTH.Normal	AUTH.Enhanced
	COM.Local via a non-IF.HumanPhysical	POE.Any	AUTH.Normal	AUTH.Normal	AUTH.Enhanced
	COM.Adjacent via IF.Any		AUTH.Normal	AUTH.Normal	AUTH.Enhanced
	COM.Public via IF.Any		AUTH.Normal	AUTH.Enhanced	AUTH.Enhanced

900 For protection measures that are labelled with [*] it is not required that the SHPSF uses authentication mechanisms for
 901 its following functions:

- 902 • factory reset function

903 5.1.3.3 [AUTHZ-LP] Least privilege in authorization policies

904 The SHPSF shall use an authorization policy that only grants permissions that are necessary for the intended purpose.

905 NOTE: A SHPSF whose intended purpose justifies not to differentiate between different user roles, can grant all
 906 necessary permissions to the user.

907 5.1.3.4 [AUTHZ-R] Revocability of granted permissions

908 The SHPSF shall support the revocation of any permission granted by an authorized entity.

909 EXAMPLE: An administrative user can revoke permissions granted to another user.

910 5.1.4 Integrity protection

911 5.1.4.1 [INT-SWPCK] Software package verification

912 The SHPSF shall use software package verification mechanisms to verify the integrity and authenticity of software
 913 packages prior to installation where the software package verification mechanism's strength levels are specified in
 914 clause [E.2.1](#) and where the minimal software package verification mechanism's strength is determined by table [4](#).

915 NOTE: The requirement addresses software packages that are updates and new software to be installed.

916 **Table 4: Assignment of the software package verification mechanism's strength levels for the**
 917 **verification of software packages**

		Highest IMP.INT of the SHPSF's integrity relevant functions		
		IMP.INT.Low	IMP.INT.Medium	IMP.INT.High
Attack Surface determined by the COM of the architectural	COM.StrictLocal	INT.SW.VER.Basic	INT.SW.VER.Basic	INT.SW.VER.Basic
	COM.Local, COM.Adjacent or COM.Public	INT.SW.VER.Normal	INT.SW.VER.Normal	INT.SW.VER.Enhanced

918 5.1.4.2 [INT-COM] Communication of integrity relevant data

919 The SHPSF shall use integrity protecting communication mechanisms to protect the integrity of communicated integrity
920 relevant data, where the corresponding integrity protection measures strengths are specified in clause [E.2.2](#) and the
921 minimal required integrity protection measures' strength are determined by table [5](#).

922 **Table 5: Assignment of protection mechanisms strength level for the integrity protection of outgoing**
923 **data and for the integrity verification of incoming data.**

			Integrity relevant data impact class		
			IMP.INT.Low	IMP.INT.Medium	IMP.INT.High
Attack Surface determined by COM, IF and POE of the architectural component that communicates integrity relevant data	COM.StrictLocal via IF.Machine	POE.Any	INT.COM.Basic	INT.COM.Basic	INT.COM.Basic
	COM.Local via IF.Machine or IF.HumanLogical	POE.FullyControlled	INT.COM.Basic	INT.COM.Basic	INT.COM.Normal
		POE.PartiallyControlled	INT.COM.Basic	INT.COM.Normal	INT.COM.Enhanced
		POE.Mobile	INT.COM.Basic	INT.COM.Normal	INT.COM.Enhanced
	COM.Adjacent via IF.Any	POE.Any	INT.COM.Enhanced	INT.COM.Enhanced	INT.COM.Enhanced
	COM.Public via IF.Any		INT.COM.Enhanced	INT.COM.Enhanced	INT.COM.Enhanced

924 5.1.5 Confidentiality protection

925 5.1.5.1 [CONF-SSM] Confidentiality protecting persistent storage for confidential 926 data

927 The SHPSF shall use confidentiality protecting secure storage mechanisms for persistently stored confidential data,
928 where the mechanisms' strength are specified in clause [E.3.1](#) and the minimal required mechanisms' strength are
929 determined by table [6](#).

930 **Table 6: Assignment for confidentiality protecting secure storage mechanisms**

		Confidentiality impact class for persistently stored confidential data		
		IMP.CONF.Low	IMP.CONF.Medium	IMP.CONF.High
Attack Surface determined by POE of the architectural	POE.FullyControlled	N/A	N/A	N/A
	POE.PartiallyControlled	N/A	CONF.SSM.Basic[*]	CONF.SSM.Normal
	POE.Mobile	CONF.SSM.Basic[*]	CONF.SSM.Normal	CONF.SSM.Enhanced

931 For protection measures labelled with [*], it is not required that the SHPSF uses confidentiality protecting persistent
932 storage for confidential data:

- 933 • which is persistently stored on non-removable storage

934 5.1.5.2 [CONF-COM] Communication of confidential data

935 The SHPSF shall use confidentiality protecting communication mechanisms to protect the confidentiality of
936 communicated confidential data, where the corresponding confidentiality protection measures strengths are specified in
937 clause [E.3.2](#) and the minimal required confidentiality protection measures' strength are determined by table [7](#).

938 **Table 7: Assignment of protection mechanisms strength level for the confidentiality of**
939 **communicated data.**

			Confidential data impact class		
			IMP.CONF.Low	IMP.CONF.Medium	IMP.CONF.High
Attack Surface determined by COM, IF and POE of the architectural component that communicates	COM.Local via IF.Machine or IF.HumanLogical	POE.FullyControlled	N/A	N/A	CONF.COM.Normal
		POE.PartiallyControlled	N/A	CONF.COM.Basic	CONF.COM.Normal
		POE.Mobile	CONF.COM.Basic	CONF.COM.Normal	CONF.COM.Enhanced

		Confidential data impact class		
		IMP.CONF.Low	IMP.CONF.Medium	IMP.CONF.High
COM.Adjacent via IF.Any	POE.Any	CONF.COM.Enhanced	CONF.COM.Enhanced	CONF.COM.Enhanced
COM.Public via IF.Any		CONF.COM.Enhanced	CONF.COM.Enhanced	CONF.COM.Enhanced

940 5.1.6 Data minimization

941 5.1.6.1 [DMIN-DJST] Documented justification of processed data

942 The SHPSF shall only process confidential data according to its intended purpose.

943 EXAMPLE: The SHPSF provides documentation that specifies the conditions under which audio or video data
944 is captured, stored, or transmitted when connected to the intended purpose. The data is processed
945 only in the cases specified in the documentation.

946 5.1.7 Availability protection

947 5.1.7.1 [AVAI-TIME-RECO-POW] Restoration after loss of power

948 A hardware architectural component shall use a mechanism to resume connectivity and functionality in the case of a
949 loss of power as soon as the power supply is restored.

950 5.1.7.2 [AVAI-TIME-NETW] Local operation

951 Where network connectivity is not necessary for a time sensitive function to operate, the SHPSF shall ensure that local
952 operability of this function is supported in case of a loss of network access.

953 5.1.7.3 [AVAI-TIME-RECO-NETW] Restoration after loss of network connection

954 The SHPSF shall use a mechanism to attempt to reconnect cleanly after a loss of network connection.

955 EXAMPLE: A SHPSF loses connection to the local network as the network is temporarily unavailable. After
956 recognizing the restored network, the SHPSF reconnects after a randomized delay to reconnect
957 cleanly.

958 NOTE 1: *Reconnecting cleanly* normally involves resuming connectivity to network in an expected, operational
959 and stable state and in an orderly fashion taking the capability of the infrastructure into consideration.

960 NOTE 2: In scenarios where continuous operational functionality is of higher priority than restoring network
961 connectivity, trade-off of number of attempts and intervals between attempts can be justified.

962 5.1.7.4 [AVAI-TIME-OUTA-NOT] Notify non-availability

963 Where at least one time sensitive function with IMP.AVAI.TIME.Medium or higher is provided by the SHPSF, the
964 SHPSF shall use a mechanism to warn the user before or at least during a IMP.AVAI.TIME.Medium or higher function
965 becomes unavailable due to loss of network connection or imminent loss of power.

966 EXAMPLE: A cloud RDPS recognises a non-availability of its MP and sends a notification to the user.

967 NOTE: A mechanism to warn the user cannot ensure that the user receives the warning. For example, a SHPSF
968 with only local communication connectivity placed in a summer house may run out of battery before the
969 user warning is delivered. However, the user would have been warned when being present before battery
970 exhaustion.

971 5.1.7.5 [AVAI-TIME-PREV-NOT] Notify upcoming limitation

972 Where at least one time sensitive function with IMP.AVAI.TIME.High is provided by the SHPSF, the SHPSF shall use
973 a mechanism to notify the user before the hardware architectural component restrains the use of power when the SHPSF
974 recognises low power condition.

975 EXAMPLE: A battery powered SHPSF recognizes low battery and sends a notification to the user.

976 NOTE: A mechanism to notify the user cannot ensure that the user receives the notification.

977 5.1.7.6 [AVAI-TIME-NET-PRIO] Network prioritization

978 Where at least one time sensitive function with IMP.AVAI.TIME.Medium or higher with the need of network
979 connectivity for its operation is provided by the SHPSF, the SHPSF shall use a mechanism to prioritize its use of
980 network resources in case of a network resource conflict:

- 981 • such that these functions are prioritized according to their IMP.AVAI.TIME.High; or
- 982 • such that functions are prioritized according to user decisions or configuration.

983 5.1.7.7 [AVAI-TIME-RES-PRIO] Power resource prioritization

984 Where

- 985 • at least one time sensitive function with IMP.AVAI.TIME.Medium or higher is provided by the SHPSF; and
- 986 • the SHPSF is intended to be powered by battery,

987 the SHPSF shall use a mechanism to prioritize use of power in the case of a low power condition:

- 988 • such that these functions are prioritized according to their IMP.AVAI.TIME; or
- 989 • such that functions are prioritized according to user decisions or configuration.

990 5.1.7.8 [AVAI-TIME-IMP-AMP] Amplification control

991 Where at least one function, whose use can impact the availability of other devices, services or networks with
992 IMP.FH.DSN.Medium or higher is provided by the SHPSF, the SHPSF shall use mechanisms to prevent effective
993 amplification of requests or network traffic of these functions.

994 EXAMPLE: An ICMP request has an amplification factor of three. Then the response time is artificially
995 extended by a factor of tree per destination to have no effective gain in bandwidth.

996 5.1.7.9 [AVAI-TIME-DOS-RATE] Incoming rate limiting

997 Where at least one time sensitive function with IMP.AVAI.TIME.High AND at least one machine interface are
998 provided by the SHPSF, the SHPSF shall use mechanisms to discard packets from a source if it sends an unusually high
999 number of requests, whose execution could result in a resource conflict.

1000 5.1.7.10 [AVAI-SUM-SCHEDULE] Scheduling of updates

1001 Where

- 1002 • the SHPSF has the capability to connect to a public network; and
- 1003 • at least one time sensitive function with IMP.AVAI.TIME.Medium or higher is provided by an architectural
1004 component,

1005 the SHPSF shall support the scheduling of the application of updates of those architectural components.

1006 5.1.8 Impact minimization

1007 5.1.9 Limit attack surface

1008 5.1.9.1 [LAS-INVAL] Validation of external data input

1009 The SHPSF shall use input validation mechanisms for all external data input received via:

- 1010 • COM.Local;
- 1011 • COM.Adjacent; and
- 1012 • COM.Public.

1013 EXAMPLE: If an application expects the input to be an email address, any input that does not conform to the
1014 format of an e-mail address will be rejected.

1015 NOTE 1: The specific pattern to accept external data input depends amongst others on the manner the external data
1016 input is intended to be processed. This means that an acceptance pattern for broad purposes (such as
1017 administration via a "Secure Shell") is typically less specific than an acceptance pattern for a specific
1018 purpose (such as a measurement value of a specific format to be stored).

1019 NOTE 2: Typically the validation of different parts of the input will happen at different layers. Network layer of the
1020 operating system verify only information relevant to the network. An application verifies only input that
1021 is relevant to that application.

1022 5.1.9.2 [LAS-INSAN] Sanitization of external data input

1023 The SHPSF shall use input sanitization mechanisms at application layer before using external data input, where the
1024 validation of external data input cannot prevent potential incidents triggered by the external data input.

1025 EXAMPLE: If external data input is amongst others intended to be stored via a database service, escape
1026 characters and other database service specific commands (defined by a corresponding function
1027 specific pattern) are removed from the external data input, before it is processed by the database
1028 service.

1029 5.1.9.3 [LAS-PHY-INF] Only necessary physical interfaces

1030 hardware architectural components shall only provide physical interfaces, that are necessary for the SHPSF's intended
1031 purpose.

1032 5.1.9.4 [LAS-LOGIC-INF] Only necessary logical interfaces active by default

1033 The SHPSF shall by default only provide logical interfaces, that are necessary for its intended purpose.

1034 5.1.9.5 [LAS-APP] Only necessary apps by default

1035 The SHPSF shall by default only provide installed application software, that are necessary for its intended purpose.

1036 5.1.9.6 [LAS-SBOOT] Secure boot

1037 Where at least one function, whose use can cause harm with IMP.FH.High is provided by the SHPSF and the SHPSF
1038 includes hardware architectural components, the hardware architectural components shall use a bootloader function that
1039 only executes core software at startup, whose integrity and authenticity is verified.

1040 NOTE: The requirement corresponds to the verified boot capability in ETSI EN 304 623 vx.x.x [i.5]

1041 5.1.10 Logging and monitoring mechanisms

1042 5.1.10.1 [LOG-LOW] Events to log for low risk SHPSF

1043 Where the SHPSF has a function, whose use can cause harm of impact class low as its highest function impact class, the
1044 SHPSF shall support logging mechanisms to create audit events for every:

- 1045 • change of configuration affecting core software;
- 1046 • starts, shutdowns or other changes of operational states of core software;
- 1047 • errors of the core software.

1048 5.1.10.2 [LOG-MEDIUM] Events to log for medium risk SHPSF

1049 Where the SHPSF has a function, whose use can cause harm of impact class medium as its highest function impact
1050 class, the SHPSF shall use logging mechanisms to create audit events for every:

- 1051 • unsuccessful authentication attempt;
- 1052 • change of configuration affecting core software;

- 1053 • starts, shutdowns or other changes of operational states of core software;
- 1054 • errors of the core software;
- 1055 • unsuccessful attempt of an identity to gain additional privileges;
- 1056 • unsuccessful attempt of an identity to access a data asset or function asset .

1057 5.1.10.3 [LOG-HIGH] Events to log for high risk SHPSF

1058 Where the SHPSF has a function, whose use can cause harm of impact class high as its highest function impact class,
1059 the SHPSF shall use logging mechanisms to create audit events for every:

- 1060 • every authentication attempt;
- 1061 • change of configuration affecting core software;
- 1062 • starts, shutdowns or other changes of operational states of core software;
- 1063 • change of configuration affecting application software whom realize function, whose use can cause harm of
1064 impact class high;
- 1065 • starts, shutdowns or other changes of operational states of application software whom realize function, whose
1066 use can cause harm of impact class high;
- 1067 • errors of the core software;
- 1068 • errors of the application software whom realize function, whose use can cause harm of impact class high;
- 1069 • every attempt of an identity to gain additional privileges;
- 1070 • every attempt of an identity to access a data asset or function asset .

1071 5.1.10.4 [LOG-TIME] Timestamps for logs

1072 Where the SHPSF does not has a function, whose use can cause harm of impact class high, the SHPSF shall use at least
1073 a time service or function to include a timestamp in every audit event, created by the SHPSF.

1074 5.1.10.5 [LOG-TIME-HIGH] Real-Timestamps for logs

1075 Where the SHPSF has a function, whose use can cause harm of impact class high as its highest function impact class,
1076 the SHPSF shall use a real-time service or clock to include a real-time timestamp in every audit event, created by the
1077 SHPSF.

1078 5.1.10.6 [LOG-STORAGE] Persistently store logfiles

1079 Where the SHPSF has a function, whose use can cause harm of impact class medium or higher as its highest function
1080 impact class, the SHPSF shall use integrity protecting secure storage mechanisms to store every audit event created by
1081 the SHPSF persistently.

1082 5.1.10.7 [LOG-BACKUP] Backup of logfiles

1083 Where the SHPSF has a function, whose use can cause harm of impact class high as its highest function impact class,
1084 the SHPSF shall automatically backup its audit events to another device or another part of the SHPSF that is in another
1085 physical location.

1086 5.1.11 Deletion mechanisms

1087 5.1.11.1 [DLM-PERM] Permanent removal of user-related data

1088 The SHPSF shall provide at least one deletion mechanism that:

- 1089 • allows a user to permanently remove its user-related data, user-installed applications, including subsets of
1090 those; and

- 1091 • is easy to use.

1092 NOTE: This requirement differs mainly from [SDC-FRM] as [DLM-PERM] allows to delete single data assets.

1093 5.1.12 Other product's technical requirements specifications

1094 5.1.12.1 [USERNOT-NOSECFUC] User notifications on not available security 1095 functions

1096 The SHPSF shall notify a user when security functions that are supposed to be used or supported by the SHPSF are not
1097 available.

1098 5.1.12.2 [USERNOT-SECREL] Language and representation for security-related user 1099 notifications

1100 Where the SHPSF is intended to be installed or maintained by a consumer for private usage, the SHPSF shall use user
1101 notification mechanisms for security-related notifications that:

- 1102 • use a language that is clear, understandable, intelligible, legible and can be easily understood by users for
1103 security-related notifications; and
- 1104 • clearly distinguish the representation of security-related notifications from other notifications.

1105 5.1.12.3 [GUI-SECCONF] Visual representation of security-related configuration via 1106 GUIs

1107 Where the SHPSF is intended to be installed or maintained by a consumer for private usage, and the SHPSF provides a
1108 GUI for security-related configuration functionality, the SHPSF shall ensure that those GUIs:

- 1109 • clearly distinguish security-related configuration options visually from other configuration options; and
- 1110 • clearly communicate the security-related consequences of changing each security-related configuration option
1111 in a language that is clear, understandable, intelligible, legible and can be easily understood by users; and
- 1112 • clearly highlight visually when changes to security-related configuration are made by a user.

1113 5.1.12.4 [CRY-SOTA] State-of-the-art cryptography

1114 The SHPSF shall by default only use cryptographic algorithms for cryptographic functions that are

- 1115 • listed in Agreed Cryptographic Mechanisms [2]; or
- 1116 • suitable for the corresponding use.

1117 5.1.12.5 [CRY-CCK-PRE-LEN] Key size of preinstalled confidential cryptographic 1118 keys

1119 The SHPSF shall only provide preinstalled confidential cryptographic keys of key sizes that are

- 1120 • listed in Agreed Cryptographic Mechanisms [2]; or
- 1121 • provide a minimum security strength of 112 bits.

1122 5.1.12.6 [CRY-CCK-GEN] Default key size of generated confidential cryptographic 1123 keys

1124 The SHPSF shall by default only generate confidential cryptographic keys of key sizes that are

- 1125 • listed in Agreed Cryptographic Mechanisms [2]; or provide a minimum security strength of 112 bits.

1126 5.1.12.7 [CRY-PW-PRE-COM] Complexity of preinstalled passwords

1127 The SHPSF shall only provide preinstalled passwords:

- 1128 • that meet the minimal recommended password complexity $C_{\{PW,min\}}$ determined by the corresponding
 1129 authentication mechanisms' usage according to table 3, and
- 1130 • that are either
- 1131 - individual per SHPSF and not derivable via public available information or
- 1132 - random per SHPSF.

1133 5.1.12.8 [CRY-PW-GEN-COM] Default complexity of generated passwords

1134 The SHPSF shall by default only generate passwords:

1135 of minimal recommended password complexity $C_{\{PW,min\}}$ determined by the corresponding authentication
 1136 mechanisms' usage according to table 3 and that are random.

1137 5.1.12.9 [CRY-PW-USR-COM] Recommended complexity of user chosen passwords

1138 The SHPSF shall only use user chosen passwords of minimal recommended password complexity $C_{\{PW,min\}}$
 1139 determined by the corresponding authentication mechanisms' usage according table 3, except for user chosen passwords
 1140 where the user explicitly confirms their usage after a warning by the SHPSF.

1141 5.2 Requirements specifications for vulnerability handling 1142 activities related to the product

1143 The requirements specified in CEN/CLC JT013090:2026 (CEN/CLC prEN 40000-1-3) [1] shall be fulfilled for the
 1144 SHPSF.

1145 6 Assessing for compliance with requirements

1146 6.1 Assessing for compliance with product's technical 1147 requirements specifications

1148 6.1.1 General

1149 In order to assess the compliance with the requirements listed in clause 5.1 of the present document, the assessment
 1150 procedures described in clause 6.1 are to be followed. When performing assessments, the distribution of security
 1151 functions (see clause 4.5) are to be considered, including whether the product provides security functions itself,
 1152 demands them from other products with digital elements within its context, or supplies them to other products with
 1153 digital elements.

1154 If there are already existing evidences (e.g. provided by manufacturers of components that are integrated in the SHPSF)
 1155 that:

- 1156 • are covering the same assessment activities as described in clause 6.1, and
- 1157 • are valid for the moment of the assessment to be performed under clause 6.1,

1158 those existing evidences can be used for the "assignment of verdict" and as "supporting evidence".

1159 6.1.2 Known exploitable vulnerabilities

1160 6.1.2.1 Assessment criteria for [NKEV-SUM-SUPPORT]

1161 **Assessment objective:**

1162 The assessment covers:

- 1163 • a conceptual assessment of [NKEV-SUM-SUPPORT],

- 1164 • a functional completeness assessment on the SHPSF's capabilities that are addressed by
1165 [NKEV-SUM-SUPPORT]
- 1166 • a functional sufficiency assessment of each software update mechanism used by the SHPSF to fulfil
1167 [NKEV-SUM-SUPPORT]
- 1168 based on the default configuration required by clause [5.1.2](#).
- 1169 **Assessment preparation:**
- 1170 The following documentation for the SHPSF shall be complete:
- 1171 • a list of all software architectural components of the SHPSF,
1172 • a list of software architectural components declared immutable, including technical justification,
1173 • documentation describing all supported software update mechanisms, including:
1174 - their scope, and
1175 - interfaces through which updates can be invoked.
- 1176 The following test setups shall be prepared:
- 1177 • a test setup that allows to identify software update mechanisms on a sample SHPSF in default configuration;
1178 • for each software update mechanism, a test setup that allows to perform an update over that software update
1179 mechanism
- 1180 **Assessment activities:**
- 1181 The following activities shall be performed:
- 1182 • The SHPSF's conformity to [NKEV-SUM-SUPPORT] shall be validated based on the documentation.
1183 • The correctness and completeness of the documentation shall be verified by:
1184 - inspecting the SHPSF to identify software architectural components, e.g. by generating SBOMs
1185 - whether each identified component is associated with a documented update path.
1186 • For each software update mechanism, its correct implementation shall be verified by:
1187 - installing an update over this software update mechanism to update a software architectural component
1188 and
1189 - checking whether the software has changed to the updated software.
- 1190 **Assignment of verdict:**
- 1191 The verdict PASS shall be assigned if:
- 1192 • the documentation indicates the SHPSF's conformity with [NKEV-SUM-SUPPORT]; and
1193 • the verification of the correctness and completeness of the documentation was successful; and
1194 • the verification of the correct implementation of each software update mechanism was successful.
- 1195 The verdict FAIL shall be assigned otherwise.
- 1196 **Supporting Evidence:**
- 1197 • records of the validation of the documentation
1198 • descriptions of the performed tests and records of performed tests to verify the correctness and completeness
1199 of the documentation

- 1200 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each
1201 software update mechanism

1202 6.1.2.2 Assessment criteria for [NKEV-SUM-PROVIDE]

1203 **Assessment objective:**

1204 The assessment covers:

- 1205 • a conceptual assessment of [NKEV-SUM-PROVIDE],
- 1206 • a functional completeness assessment on the capabilities of the SHPSF's architectural components that are
1207 addressed by [NKEV-SUM-PROVIDE]
- 1208 • a functional sufficiency assessment of each software update mechanism provided by the SHPSF's architectural
1209 components to fulfil [NKEV-SUM-PROVIDE]

1210 based on the default configuration required by clause [5.1.2](#).

1211 **Assessment preparation:**

1212 The following documentation for the SHPSF shall be complete:

- 1213 • a list of all architectural components of the SHPSF that include core software,
- 1214 • a list of architectural components declared immutable, including technical justification,
- 1215 • documentation describing all provided software update mechanisms, including:
- 1216 - their scope, and
- 1217 - interfaces through which updates can be invoked.

1218 The following test setups shall be prepared:

- 1219 • a test setup that allows to identify software update mechanisms on sample architectural components of the
1220 SHPSF in default configuration;
- 1221 • for each software update mechanism, a test setup that allows to perform an update over that software update
1222 mechanism

1223 **Assessment activities:**

1224 The following activities shall be performed:

- 1225 • The SHPSF's conformity to [NKEV-SUM-PROVIDE] shall be validated based on the documentation.
- 1226 • The correctness and completeness of the documentation shall be verified by:
- 1227 - inspecting the architectural components of the SHPSF that include core software and
- 1228 - checking whether each identified component is associated with a documented update path.
- 1229 • For each software update mechanism, its correct implementation shall be verified by:
- 1230 - installing an update over this software update mechanism to update a software architectural component
1231 and
- 1232 - checking whether the software has changed to the updated software.

1233 **Assignment of verdict:**

1234 The verdict PASS shall be assigned if:

- 1235 • the documentation indicates the SHPSF's conformity with [NKEV-SUM-PROVIDE]; and

- 1236 • the verification of the correctness and completeness of the documentation was successful; and
- 1237 • the verification of the correct implementation of each software update mechanism was successful.

1238 The verdict FAIL shall be assigned otherwise.

1239 **Supporting Evidence:**

- 1240 • records of the validation of the documentation
- 1241 • descriptions of the performed tests and records of performed tests to verify the correctness and completeness
- 1242 of the documentation
- 1243 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each
- 1244 software update mechanism

1245 **6.1.2.3 Assessment criteria for [NKEV-SUM-AUTO]**

1246 **Assessment objective:**

1247 The assessment covers:

- 1248 • a conceptual assessment of [NKEV-SUM-AUTO],
- 1249 • a functional sufficiency assessment of each software update mechanism used by the SHPSF to fulfil
- 1250 [NKEV-SUM-AUTO]

1251 based on the default configuration required by clause [5.1.2](#).

1252 **Assessment preparation:**

1253 The following documentation for the SHPSF shall be complete:

- 1254 • documentation describing all supported software update mechanism, including:
 - 1255 - their scope,
 - 1256 - interfaces through which updates can be invoked, and
 - 1257 - their capability to perform automatic updates

1258 The following test setups shall be prepared:

- 1259 • for each software update mechanism, a test setup that ensures internet-connectivity and that allows to perform
- 1260 an automatic update over that software update mechanism

1261 **Assessment activities:**

1262 The following activities shall be performed:

- 1263 • The SHPSF's conformity to [NKEV-SUM-AUTO] shall be validated based on the documentation.
- 1264 • For each software update mechanism, its correct implementation shall be verified by:
 - 1265 - installing an automatic update with internet connection over this software update mechanism to update a
 - 1266 software architectural component,
 - 1267 - checking whether the product performs the automatic update without human intervention at the product
 - 1268 or via scheduling the installation under human approval or via triggering the installation under human
 - 1269 approval, and
 - 1270 - checking whether the software version has been updated to a new version.

1271 **Assignment of verdict:**

1272 The verdict PASS shall be assigned if:

- 1273 • the documentation indicates the SHPSF's conformity with [NKEV-SUM-AUTO] and
- 1274 • the verification of the correct implementation of each software update mechanism was successful.

1275 The verdict FAIL shall be assigned otherwise.

1276 **Supporting Evidence:**

- 1277 • records of the validation of the documentation
- 1278 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each
- 1279 software update mechanism

1280 **6.1.2.4 Assessment criteria for [NKEV-SUM-NOTIF]**

1281 **Assessment objective:**

1282 The assessment covers:

- 1283 • a conceptual assessment of [NKEV-SUM-NOTIF],
- 1284 • a functional completeness assessment on the SHPSF's capabilities that are addressed by [NKEV-SUM-NOTIF]
- 1285 • a functional sufficiency assessment of each software update notification mechanism used by the SHPSF to
- 1286 fulfil [NKEV-SUM-NOTIF]

1287 based on the default configuration required by clause [5.1.2](#).

1288 **Assessment preparation:**

1289 The following documentation for the SHPSF shall be complete:

- 1290 • documentation describing all supported software update notification mechanisms, including:
 - 1291 - how the software update notification is performed, and
 - 1292 - to what extent this software update notification is automated.

1293 The following test setups shall be prepared:

- 1294 • a test setup that allows to identify software update notification mechanisms on a sample SHPSF in default
- 1295 configuration;
- 1296 • for each software update notification mechanism, a test setup that allows to make software updates available
- 1297 and therefore to trigger the notification

1298 **Assessment activities:**

1299 The following activities shall be performed:

- 1300 • The SHPSF's conformity to [NKEV-SUM-NOTIF] shall be validated based on the documentation.
- 1301 • The correctness and completeness of the documentation shall be verified by:
 - 1302 - inspecting the SHPSF to identify software update notification mechanisms.
- 1303 • For each software update notification mechanism, its correct implementation shall be verified by:
 - 1304 - making a software update available at the source holding security updates and
 - 1305 - checking whether the software update notification mechanism automatically notifies the SHPSF's users
 - 1306 that an update of its software is available

1307 **Assignment of verdict:**

1308 The verdict PASS shall be assigned if:

- 1309 • the documentation indicates the SHPSF's conformity with [NKEV-SUM-NOTIF]; and
- 1310 • the verification of the correctness and completeness of the documentation was successful; and
- 1311 • the verification of the correct implementation of each software update notification mechanism was successful.

1312 The verdict FAIL shall be assigned otherwise.

1313 **Supporting Evidence:**

- 1314 • records of the validation of the documentation
- 1315 • descriptions of the performed tests and records of performed tests to verify the correctness and completeness
- 1316 of the documentation
- 1317 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each
- 1318 software update notification mechanism

1319 6.1.3 Default configuration

1320 6.1.3.1 Assessment criteria for [SDC-AUM-FH]

1321 **Assessment objective:**

1322 The assessment covers:

- 1323 • a conceptual assessment of [SDC-AUM-FH];
- 1324 • a functional completeness assessment on the SHPSF capabilities that are addressed by [SDC-AUM-FH];

1325 based on the factory default state.

1326 NOTE: A functional sufficiency assessment of each authentication mechanism used by the SHPSF to fulfil
1327 [SDC-AUM-FH] is addressed by the assessment of [AUM-FH].

1328 **Assessment preparation:**

1329 The following documentation for the SHPSF shall be complete:

- 1330 • a list of SHPSF's functions whose use can cause harm that are enabled in the factory default state or can be
- 1331 activated during initialisation.
- 1332 - the physical operational environment of the architectural component that performs the function;
- 1333 - for each of the function's trigger input possibilities:
 - 1334 ▪ the interface and communication type;
 - 1335 ▪ a list of corresponding authentication mechanisms including:
 - 1336 • the authentication mechanisms' strength;

1337 NOTE: This documentation is a subset of the documentation required for the assessment of [AUM-FH]

1338 The following test setups shall be prepared:

- 1339 • a test setup for identifying functions, their trigger input possibilities and corresponding authentication
- 1340 mechanisms based on a sample SHPSF in factory default state and after initialisation

1341 **Assessment activities:**

- 1342 • The SHPSF's conformity to [SDC-AUM-FH] shall be validated based on the documentation.
- 1343 • The correctness and completeness of the documentation shall be verified by:

- 1344 - inspecting the SHPSF in factory default state; and
- 1345 - (if functions whose use can cause harm can be configured during initialisation) performing the
- 1346 initialisation without providing explicit confirmation of configurations deviating from the minimal
- 1347 required authentication strength determined by table 3 and inspecting the SHPSF after initialisation.

1348 **Assignment of verdict:**

1349 The verdict PASS shall be assigned if:

- 1350 • the documentation indicates the SHPSF's conformity to [SDC-AUM-FH]; and
- 1351 • the verification of the correctness and completeness of the documentation was successful

1352 The verdict FAIL shall be assigned otherwise.

1353 **Supporting Evidence:**

- 1354 • records of the validation of the documentation;
- 1355 • descriptions of the performed tests and records of performed tests to verify the correctness and completeness
- 1356 of the documentation.

1357 **6.1.3.2 Assessment criteria for [SDC-FRM]**

1358 **Assessment objective:**

1359 The assessment functionally determines whether all user-related data, installed applications, and configurations

1360 deviating from the default state are erased after using the factory reset mechanism.

1361 **Assessment preparation:**

- 1362 • Documentation on how the factory reset mechanism can be accessed.
- 1363 • The SHPSF shall be set up and some configuration changes shall be created and persistently stored.
- 1364 • Where the SHPSF supports the storage of user-related data, some user-related data shall be created and
- 1365 persistently stored on the SHPSF.
- 1366 • Where the SHPSF supports the installation of applications, some common application for the SHPSF shall be
- 1367 installed.

1368 NOTE: User-related data also encompasses cryptographic keys, e.g. Wi-Fi® passwords, certificates.

1369 **Assessment activities:**

- 1370 • An authorised entity shall start the factory reset mechanism.
- 1371 • The erasure of user-related data, applications and configurations shall be validated:
- 1372 - The restoration of the device settings to their default state shall be validated.
- 1373 • Attempts to access any previous user accounts or data shall be made.

1374 **Assignment of verdict:**

1375 The verdict PASS shall be assigned when all user-related data, installed applications, and configurations deviating from

1376 the default state are erased

1377 The verdict FAIL shall be assigned otherwise.

1378 **Supporting Evidence:**

- 1379 • Description of the performed test
- 1380 • All test records of the performed test

1381 6.1.4 Authentication and access control mechanisms

1382 6.1.4.1 Assessment criteria for [ACM-FH]

1383 **Assessment objective:**

1384 The assessment covers:

- 1385 • a conceptual assessment of [ACM-FH];
- 1386 • a functional completeness assessment on the SHPSF capabilities that are addressed by [ACM-FH];
- 1387 • a functional sufficiency assessment of each access control mechanism used by the SHPSF to fulfil [ACM-FH]

1388 based on the default configuration required by clause [5.1.2](#).

1389 **Assessment preparation:**

1390 The following documentation for the SHPSF shall be complete:

- 1391 • a list of SHPSF's functions whose use can cause harm;
- 1392 • for each function, whose use can cause harm:
 - 1393 - its impact class impact class for function, whose use can cause harm;
 - 1394 - the physical operational environment of the architectural component that performs the function;
 - 1395 - for each of the function's trigger input possibilities:
 - 1396 ▪ the interface and communication type;
 - 1397 ▪ a list of corresponding access control mechanisms including their default authorization policy.

1398 The following test setups shall be prepared:

- 1399 • a test setup for identifying functions, their trigger input possibilities and corresponding access control
1400 mechanisms based on a sample SHPSF in default configuration;
- 1401 • for each access control mechanism, a test setup that allows privilege escalation attacks from authenticated
1402 entities and unauthorized access attempts of unauthenticated entities.

1403 **Assessment activities:**

- 1404 • The SHPSF's conformity to [ACM-FH] shall be validated based on the documentation.
- 1405 • The correctness and completeness of the documentation shall be verified by:
 - 1406 - an inspection of the SHPSF for functions and related access control mechanisms that are accessible via
1407 physical human interfaces;
 - 1408 - a scan of the SHPSF for functions and related access control mechanisms that are accessible via logical
1409 interfaces.
- 1410 • For each access control mechanism, its correct implementation shall be verified based on attempts to violate
1411 the authorization policy by:
 - 1412 - privilege escalation of authenticated entities based on the default authorization policy;
 - 1413 - unauthorized usage of function, whose use can cause harm by unauthenticated entities based on the
1414 default authorization policy.

1415 **Assignment of verdict:**

1416 The verdict PASS shall be assigned if:

- 1417 • the documentation indicates the SHPSF's conformity to [ACM-FH]; and
- 1418 • the verification of the correctness and completeness of the documentation was successful; and
- 1419 • the verification of the correct implementation of each access control mechanism was successful.

1420 The verdict FAIL shall be assigned otherwise.

1421 **Supporting Evidence:**

- 1422 • records of the validation of the documentation;
- 1423 • descriptions of the performed tests and records of performed tests to verify the correctness and completeness
- 1424 of the documentation;
- 1425 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each
- 1426 access control mechanism

1427 **6.1.4.2 Assessment criteria for [AUM-FH]**

1428 **Assessment objective:**

1429 The assessment covers:

- 1430 • a conceptual assessment of [AUM-FH];
 - 1431 • a functional completeness assessment on the SHPSF capabilities that are addressed by [AUM-FH];
 - 1432 • a functional sufficiency assessment of each authentication mechanism used by the SHPSF to fulfil [AUM-FH]
- 1433 based on the default configuration required by clause [5.1.2](#).

1434 **Assessment preparation:**

1435 The following documentation for the SHPSF shall be complete:

- 1436 • a list of SHPSF's functions whose use can cause harm
- 1437 • for each function, whose use can cause harm:
 - 1438 - its impact class impact class for function, whose use can cause harm;
 - 1439 - the physical operational environment of the architectural component that performs the function;
 - 1440 - for each of the function's trigger input possibilities:
 - 1441 ▪ the interface and communication type;
 - 1442 ▪ a list of corresponding authentication mechanisms including:
 - 1443 • the authentication mechanisms' strength;
 - 1444 • the type of authentication factors.

1445 The following test setups shall be prepared:

- 1446 • a test setup for identifying functions, their trigger input possibilities and corresponding authentication
- 1447 mechanisms based on a sample SHPSF in default configuration;
- 1448 • for each authentication mechanism, a test setup defined by the test cases provided in clause [E.1](#) according to
- 1449 the needs determined by its strength and the type of its authentication factors.

1450 **Assessment activities:**

- 1451 • The SHPSF's conformity to [AUM-FH] shall be validated based on the documentation.

- 1452 • The correctness and completeness of the documentation shall be verified by:
- 1453 - an inspection of the SHPSF for functions and related authentication mechanisms that are accessible via
- 1454 physical human interfaces;
- 1455 - a scan of the SHPSF for functions and related authentication mechanisms that are accessible via logical
- 1456 interfaces.
- 1457 • For each authentication mechanism, its correct implementation shall be verified based on the test cases
- 1458 provided in clause [E.1](#) according to the needs determined by its strength and the type of its authentication
- 1459 factors.

1460 **Assignment of verdict:**

1461 The verdict PASS shall be assigned if:

- 1462 • the documentation indicates the SHPSF's conformity to [AUM-FH]; and
- 1463 • the verification of the correctness and completeness of the documentation was successful; and
- 1464 • the verification of the correct implementation of each authentication mechanism was successful.

1465 The verdict FAIL shall be assigned otherwise.

1466 **Supporting Evidence:**

- 1467 • records of the validation of the documentation;
- 1468 • descriptions of the performed tests and records of performed tests to verify the correctness and completeness
- 1469 of the documentation;
- 1470 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each
- 1471 authentication mechanism.

1472 **6.1.4.3 Assessment criteria for [AUTHZ-LP]**

1473 **Assessment objective:**

1474 The assessment covers:

- 1475 • a conceptual assessment of [AUTHZ-LP].

1476 based on the default configuration required by clause [5.1.2](#)

1477 **Assessment preparation:**

1478 The following documentation for the SHPSF shall be complete:

- 1479 • a description of the authorization policies in default configuration including:
- 1480 - a list of granted permissions for entities on function, whose use can cause harm and
- 1481 - for each granted permission, a justification that it is necessary for the intended purpose.

1482 **Assessment activities:**

- 1483 • The SHPSF's conformity to [AUTHZ-LP] shall be validated based on the documentation.

1484 **Assignment of verdict:**

1485 The verdict PASS shall be assigned if:

- 1486 • the documentation indicates the SHPSF's conformity to [AUTHZ-LP].

1487 The verdict FAIL shall be assigned otherwise.

1488 **Supporting Evidence:**

- 1489 • records of the validation of the documentation

1490 **6.1.4.4 Assessment criteria for [AUTHZ-R]**

1491 **Assessment objective:**

1492 The assessment covers:

- 1493 • a functional sufficiency assessment to ensure the SHPSF supports revocation of any granted permissions.

1494 **Assessment preparation:**

1495 The following documentation for the SHPSF shall be complete:

- 1496 • a list of mechanisms to grant permissions for entities on function, whose use can cause harm.

1497 The following test setups shall be prepared:

- 1498 • for each mechanism to grant permissions, a test setup for granting and revoking permissions for entities on
1499 function, whose use can cause harm.

1500 **Assessment activities:**

- 1501 • For each mechanism to grant permissions, the revocability of grantable permissions shall be verified by:
- 1502 - granting permissions to an entity;
- 1503 - revoking the permissions; and
- 1504 - attempting use permissions after revocation.

1505 **Assignment of verdict:**

1506 The verdict PASS shall be assigned if:

- 1507 • for each mechanism to grant permissions, access is denied after revocation.

1508 The verdict FAIL shall be assigned otherwise.

1509 **Supporting Evidence:**

- 1510 • descriptions of the performed tests and records of performed tests to verify the correct implementation of
1511 [AUTHZ-R].

1512 **6.1.5 Integrity protection**

1513 **6.1.6 Confidentiality protection**

1514 **6.1.7 Data minimization**

1515 **6.1.7.1 Assessment criteria for [DMIN-DJST]**

1516 **Assessment objective:**

1517 The assessment covers:

- 1518 • a conceptual assessment of Documented justification of processed data

1519 **Assessment preparation:**

1520 The following documentation for the SHPSF shall be complete:

- 1521 • a list of all data assets processed by the SHPSF whose impact class for confidential SHPSF data is
1522 IMP.CONF.Low or higher;
- 1523 • for each documented confidential data asset, the associated rationale for its necessity explaining why its
1524 processing is necessary for the intended purpose of the SHPSF.

1525 **Assessment activities:**

- 1526 • The SHPSF's conformity to [DMIN-DJST] shall be validated based on the documentation.

1527 **Assignment of verdict:**

1528 The verdict PASS shall be assigned if:

- 1529 • the documentation indicates the SHPSF's conformity to [DMIN-DJST];

1530 Otherwise, the verdict FAIL shall be assigned.

1531 **Supporting Evidence:**

- 1532 • records of the validation of the documentation;

1533 6.1.8 Availability protection

1534 6.1.8.1 Assessment criteria for [AVAI-TIME-RECO-POW]

1535 **Assessment objective:**

1536 The assessment covers:

- 1537 • a functional sufficiency assessment of the recovery function interaction with each power supply used by the
1538 SHPSF's hardware architectural components to fulfil [AVAI-TIME-RECO-POW]

1539 based on the default configuration required by clause [5.1.2](#).

1540 **Assessment preparation:**

1541 The following documentation for the SHPSF shall be complete:

- 1542 • a list of all SHPSF's hardware architectural components:
- 1543 • for each SHPSF's hardware architectural component:
- 1544 - a list of all power supplies
- 1545 - for each power supply:
- 1546 ▪ a description whether the power supply can power the hardware architectural component alone
- 1547 - a list of all functionalities of the SHPSF that need communication involving the hardware architectural
1548 component:
- 1549 ▪ for each of these functionalities:
- 1550 • a list of interfaces of the SHPSF, where the connection status of the necessary
1551 communication channels can be read; OR
- 1552 • parameters of the necessary communication channels of the hardware architectural
1553 components in order to externally observe if the connection is active
- 1554 • a list of interfaces of the SHPSF, where the operational status of the hardware
1555 architectural components can be read:
- 1556 ○ description how the operational status can be implied from the interface
1557 readings.

1558 The following test setups shall be prepared:

- 1559 • the SHPSF is set up in default configuration
- 1560 • a test setup to:
 - 1561 - safely disconnect or disable and reconnect or enable the power supplies of the SHPSF's hardware
 - 1562 architectural components;
 - 1563 - enable access to at least one interfaces of the SHPSF, where the operational status of the SHPSF can be
 - 1564 read;
 - 1565 - enable access to at least one interfaces of the SHPSF, where the connection status the necessary
 - 1566 communication channels status of the hardware architectural components can be read;
 - 1567 - if the connection status for all necessary communication channels of the hardware architectural
 - 1568 components cannot be read from the SHPSF:
 - 1569 ▪ monitor whether all necessary communication channels of the hardware architectural components
 - 1570 are active.

1571 **Assessment activities:**

1572 The following activities shall be performed for each hardware architectural component:

- 1573 • for every possible order in which the hardware architectural component power supplies can be disconnected or
- 1574 disabled:
 - 1575 - disconnect or disable all power supplies of the hardware architectural component
 - 1576 - wait at least 30 s
 - 1577 - reconnect or enable the power supplies
 - 1578 - monitor the operational status of the SHPSF
 - 1579 - monitor the connection status for all necessary communication channels of the hardware architectural
 - 1580 component
 - 1581 - record the order in which the power supplies are disconnect or disable and reconnect or enable
 - 1582 - record the time relative to the reconnection or enabling of the last power supply, after which the SHPSF
 - 1583 indicates, that it is operational and all necessary communication channels are established; OR
 - 1584 - record the time relative to the reconnection or enabling of the last power supply, after which every
 - 1585 necessary communication channel of the hardware architectural component was active at least once, and
 - 1586 there is no indication that the SHPSF has not resumed operation

1587 **Assignment of verdict:**

1588 The verdict PASS shall be assigned if:

- 1589 • the SHPSF signals resume of operations and establishment of all necessary communication channels within
- 1590 one hour after the reconnection or enabling of the last power supply; OR
- 1591 • all necessary communication channels of the hardware architectural components were active at least once, and
- 1592 there is no indication that the SHPSF has not resumed operation within one hour
- 1593 • The verdict FAIL shall be assigned otherwise.

1594 **Supporting Evidence:**

- 1595 • descriptions of the performed tests and records of performed tests

1596 6.1.8.2 Assessment criteria for [AVAI-TIME-NETW]

1597 **Assessment objective:**

1598 The assessment covers:

- 1599 • a conceptual assessment of [AVAI-TIME-NETW];
- 1600 • a functional completeness assessment on the SHPSF capabilities that are addressed by [AVAI-TIME-NETW];
- 1601 • a functional sufficiency assessment of each time sensitive function without the need of network connectivity to
- 1602 operate used by the SHPSF to fulfil [AVAI-TIME-NETW]

1603 based on the default configuration required by clause [5.1.2](#).

1604 **Assessment preparation:**

1605 The following documentation for the SHPSF shall be complete:

- 1606 • a list of all time sensitive function of the SHPSF:
- 1607 • for each time sensitive function:
 - 1608 - description of the functionalities realised or supported by this function
 - 1609 - list of interfaces necessary for the operation of this function
 - 1610 ▪ for each interface:
 - 1611 ▪ communication types of the interface
- 1612 • a list of interfaces of the SHPSF, where the status of the architectural component's time sensitive function can
- 1613 be read
 - 1614 - description how the status can be implied from the interface readings

1615 The following test setups shall be prepared:

- 1616 • the SHPSF is set up in default configuration
- 1617 • a test setup to:
 - 1618 - disconnect or disable the public communication of the SHPSF's architectural components
 - 1619 - disconnect or disable the adjacent communication of the SHPSF's architectural components
 - 1620 - enable access to at least one interfaces of the SHPSF, where the status of the SHPSF's time sensitive
 - 1621 function can be read

1622 **Assessment activities:**

1623 The following activities shall be performed:

- 1624 • verify the correctness and completeness of the documentation
- 1625 • repeat the following steps for communication types public communication, adjacent communication and both,
- 1626 depending on the communication type needed by the functions to be tested:
 - 1627 - disconnect or disable the corresponding communication type of the SHPSF's architectural component
 - 1628 - wait at least 30 s
 - 1629 - for each time sensitive function which does not need any interface with the corresponding
 - 1630 communication type for its operation
 - 1631 ▪ check whether the function is in operable status

- 1632 ▪ record the status of the function and the disconnected or disabled communication type
- 1633 - reconnect or enable the corresponding communication type

1634 **Assignment of verdict:**

1635 The verdict PASS shall be assigned if:

- 1636 • no indication, that the documentation is incorrect or incomplete, are found
- 1637 • all checked time sensitive functions are in operable state

1638 The verdict FAIL shall be assigned otherwise.

1639 **Supporting Evidence:**

- 1640 • descriptions of the performed tests and records of performed tests

1641 **6.1.8.3 Assessment criteria for [AVAI-TIME-RECO-NETW]**

1642 **Assessment objective:**

1643 The assessment covers:

- 1644 • a conceptual assessment of [AVAI-TIME-RECO-NETW]
- 1645 • a functional completeness assessment on the SHPSF capabilities that are addressed by
- 1646 [AVAI-TIME-RECO-NETW]
- 1647 • a functional sufficiency assessment of the SHPSFs architectural components recovery after loss of network
- 1648 connection, to fulfil [AVAI-TIME-RECO-NETW]

1649 based on the default configuration required by clause [5.1.2](#).

1650 **Assessment preparation:**

1651 The following documentation for the SHPSF shall be complete:

- 1652 • a list of all functions of the SHPSF that need communication involving the architectural component
- 1653 - for each of these functions:
 - 1654 ▪ list of interfaces involving the architectural component and are necessary for the operation of this
 - 1655 function:
 - 1656 • for each interface:
 - 1657 ○ communication types of the interface
 - 1658 - a list of interfaces of the SHPSF, where the connection status of the necessary communication channels
 - 1659 can be read; OR
 - 1660 - parameters of the necessary communication channel of the architectural component in order to externally
 - 1661 observe if the connection is active

1662 The following test setups shall be prepared:

- 1663 • the SHPSF is set up in default configuration
- 1664 • a test setup to:
 - 1665 - disconnect or disable the public communication of the SHPSFs architectural component
 - 1666 - disconnect or disable the adjacent communication of the SHPSFs architectural component

- 1667 - enable access to at least one interfaces of the SHPSF, where the connection status the necessary
 1668 interfaces involving the architectural component and are necessary for the operation of these functions
 1669 can be read; OR
- 1670 - if the connection status for all necessary interfaces involving the architectural component and are
 1671 necessary for the operation of these functions cannot be read from the SHPSF:
- 1672 ▪ monitor whether all necessary interfaces involving the architectural component and are necessary
 1673 for the operation of these functions

1674 **Assessment activities:**

1675 The following activities shall be performed:

- 1676 • verify the correctness and completeness of the documentation by:
- 1677 - check for undocumented interfaces
- 1678 • repeat the following steps for communication types public communication, adjacent communication and both
 1679 at the same time:
- 1680 - disconnect or disable the corresponding communication type of the SHPSF's architectural component
- 1681 - wait at least 60s
- 1682 - reconnect or enable the corresponding communication type
- 1683 - record the corresponding communication type
- 1684 - for each documented function:
- 1685 ▪ monitor the operational status of the function
- 1686 ▪ for each interface necessary for the operation of this function:
- 1687 • monitor the connection status
- 1688 • record the time relative to the reconnection or enabling of the corresponding
 1689 communication type, after which the SHPSF indicates, that the interface is
 1690 reconnected; OR
- 1691 • record the time relative to the reconnection or enabling of the corresponding
 1692 communication type, after which the interface was active at least once, and there is
 1693 no indication that the SHPSF has not resumed operation

1694 **Assignment of verdict:**

1695 The verdict PASS shall be assigned if:

- 1696 • no indication, that the documentation is incorrect or incomplete, are found; and
- 1697 • the SHPSF signals resume of operations and establishment of all necessary communication channels within
 1698 one hour; OR
- 1699 • all necessary communication channels of the architectural component were active at least once, and there is no
 1700 indication that the SHPSF has not resumed operation within one hour
- 1701 • The verdict FAIL shall be assigned otherwise.

1702 **Supporting Evidence:**

- 1703 • descriptions of the performed tests and records of performed tests

1704 **6.1.8.4 Assessment criteria for [AVAI-TIME-OUTA-NOT]**

1705 **Assessment objective:**

1706 The assessment covers:

- 1707 • a conceptual assessment of [AVAI-TIME-OUTA-NOT]
- 1708 • a functional sufficiency assessment of the SHPSFs notification in case of non-availability induced by network
1709 resource restrictions, to fulfil [AVAI-TIME-OUTA-NOT]
- 1710 • a functional sufficiency assessment of the SHPSFs notification in case of non-availability induced by DOS, to
1711 fulfil [AVAI-TIME-PREV-NOT]

1712 based on the default configuration required by clause [5.1.2](#).

1713 **Assessment preparation:**

1714 The following documentation for the SHPSF shall be complete:

- 1715 • description how the status of the SHPSFs time sensitive functions can be read or deduced
- 1716 • a list of all time sensitive functions of the SHPSF:
 - 1717 - for each of these functions:
 - 1718 ▪ the time sensitive availability impact class
 - 1719 ▪ whether the function needs network connectivity
- 1720 • CPU, memory, power and network resources available to the SHPSF
- 1721 • demands on CPU, memory, power and network resources for workload consistent with the SHPSFs intended
1722 purpose and reasonably foreseeable use
- 1723 • a list of all notification mechanisms of the SHPSF:
 - 1724 - description how the notification mechanism can be configured

1725 The following test setups shall be prepared:

- 1726 • the SHPSF is set up in default configuration
- 1727 • configure at least one notification mechanism
- 1728 • a test setup to:
 - 1729 - limit the network bandwidth between the SHPSFs architectural component and the SHPSFs RDPS to the
1730 internet
 - 1731 - induce a denial-of-service status on the SHPSF causing increasing demand on processing resources
 - 1732 - receive notifications from the SHPSF

1733 **Assessment activities:**

1734 The following activities shall be performed:

- 1735 • verify the correctness and completeness of the documentation
- 1736 • conceptually verify whether the documented notification mechanisms are suitable to send notifications in case
1737 of resource limitations
- 1738 • if at least on time sensitive function needs network connectivity:
 - 1739 - progressively lower the network bandwidth available to the SHPSFs architectural component

- 1740 ▪ record any received notifications form the SHPSF
- 1741 - progressively higher the intensity of requests to induce a denial-of-service status on the SHPSF
- 1742 ▪ record any received notifications form the SHPSF
- 1743 **Assignment of verdict:**
- 1744 The verdict PASS shall be assigned if:
- 1745 • no indication, that the documentation is incorrect or incomplete, are found; and
- 1746 • the SHPSF sends notifications according to its configuration in case of non-availability of time sensitive
- 1747 function with IMP.AVAI.TIME.Medium or higher induced by DOS; or
- 1748 - no time sensitive function with IMP.AVAI.TIME.Medium or higher was non-availability due to DOS;
- 1749 and
- 1750 • the SHPSF sends notifications according to its configuration in case of non-availability of time sensitive
- 1751 function with IMP.AVAI.TIME.Medium or higher induced by network bandwidth limitation; or
- 1752 - no time sensitive function with IMP.AVAI.TIME.Medium or higher was non-availability due to network
- 1753 bandwidth limitation.
- 1754 The verdict FAIL shall be assigned otherwise.
- 1755 **Supporting Evidence:**
- 1756 • descriptions of the performed tests and records of performed tests
- 1757 **6.1.8.5 Assessment criteria for [AVAI-TIME-PREV-NOT]**
- 1758 **Assessment objective:**
- 1759 The assessment covers:
- 1760 • a conceptual assessment of [AVAI-TIME-PREV-NOT]
- 1761 • a functional sufficiency assessment of the SHPSFs notification in case of network resource restrictions, to
- 1762 fulfil [AVAI-TIME-PREV-NOT]
- 1763 • a functional sufficiency assessment of the SHPSFs notification in case of DOS, to fulfil
- 1764 [AVAI-TIME-PREV-NOT]
- 1765 based on the default configuration required by clause [5.1.2](#).
- 1766 **Assessment preparation:**
- 1767 The following documentation for the SHPSF shall be complete:
- 1768 • a list of all time sensitive functions of the SHPSF:
- 1769 - for each of these functions:
- 1770 ▪ the time sensitive availability impact class
- 1771 ▪ whether the function needs network connectivity
- 1772 • CPU, memory, power and network resources available to the SHPSF
- 1773 • demands on CPU, memory, power and network resources for workload consistent with the SHPSFs intended
- 1774 purpose and reasonably foreseeable use
- 1775 • a list of all notification mechanisms of the SHPSF:
- 1776 - description how the notification mechanism can be configured

1777 The following test setups shall be prepared:

- 1778 • the SHPSF is set up in default configuration
- 1779 • configure at least one notification mechanism
- 1780 • a test setup to:
 - 1781 - read or deduced the status of the time sensitive functions from the SHPSF
 - 1782 - limit the network bandwidth between the SHPSFs architectural component and the SHPSFs RDPS to the
1783 internet
 - 1784 - induce a DOS status on the SHPSF causing increasing demand on processing resources
 - 1785 - receive notifications from the SHPSF

1786 **Assessment activities:**

1787 The following activities shall be performed:

- 1788 • verify the correctness and completeness of the documentation
- 1789 • conceptually verify whether the documented notification mechanisms are suitable to send notifications in case
1790 of resource limitations
- 1791 • if at least on time sensitive function needs network connectivity:
 - 1792 - progressively lower the network bandwidth available to the SHPSFs architectural component
 - 1793 ▪ record any received notifications form the SHPSF
 - 1794 - progressively higher the intensity of requests to induce a DOS status on the SHPSF
 - 1795 ▪ record any received notifications form the SHPSF

1796 **Assignment of verdict:**

1797 The verdict PASS shall be assigned if:

- 1798 • no indication, that the documentation is incorrect or incomplete, are found; and
- 1799 • the SHPSF sends notifications according to its configuration in case of resource limitations induced by DOS;
1800 and
- 1801 • the SHPSF sends notifications according to its configuration in case of network bandwidth limitation; or
 - 1802 - no time sensitive function with IMP.AVAI.TIME.High of the SHPSF of the SHPSF needs network
1803 connectivity

1804 The verdict FAIL shall be assigned otherwise.

1805 **Supporting Evidence:**

- 1806 • descriptions of the performed tests and records of performed tests

1807 **6.1.8.6 Assessment criteria for [AVAI-TIME-NET-PRIO]**

1808 **Assessment objective:**

1809 The assessment covers:

- 1810 • a conceptual assessment of [AVAI-TIME-NET-PRIO]
- 1811 • a functional sufficiency assessment of the SHPSFs resource prioritization in case of non-availability induced
1812 by network resource restrictions, to fulfil [AVAI-TIME-NET-PRIO]

1813 based on the default configuration required by clause [5.1.2](#).

1814 **Assessment preparation:**

1815 The following documentation for the SHPSF shall be complete:

- 1816 • description how the status of the SHPSFs time sensitive functions can be read or deduced
- 1817 • a list of all time sensitive functions of the SHPSF:
 - 1818 - for each of these functions:
 - 1819 ▪ the time sensitive availability impact class
 - 1820 ▪ whether the function needs network connectivity
- 1821 • prioritization policy for the time sensitive functions of the SHPSF in case of network resource conflict

1822 The following test setups shall be prepared:

- 1823 • the SHPSF is set up in default configuration
- 1824 • a test setup to:
 - 1825 - read or deduced the status of the time sensitive functions from the SHPSF
 - 1826 - limit the network bandwidth between the SHPSFs architectural component and the SHPSFs RDPS to the
 - 1827 internet

1828 **Assessment activities:**

1829 The following activities shall be performed:

- 1830 • verify the correctness and completeness of the documentation
- 1831 • conceptually verify the prioritization policy
- 1832 • progressively lower the network bandwidth available to the SHPSFs architectural component
 - 1833 - record the status of every time sensitive function

1834 **Assignment of verdict:**

1835 The verdict PASS shall be assigned if:

- 1836 • no indication, that the documentation is incorrect or incomplete, are found; and
- 1837 • the prioritization policy is conceptually valid; and
- 1838 • the prioritization policy is represented by the status of every time sensitive function during network bandwidth
- 1839 limitation.

1840 The verdict FAIL shall be assigned otherwise.

1841 **Supporting Evidence:**

- 1842 • descriptions of the performed tests and records of performed tests

1843 **6.1.8.7 Assessment criteria for [AVAI-TIME-RES-PRIO]**

1844 **Assessment objective:**

1845 The assessment covers:

- 1846 • a conceptual assessment of [AVAI-TIME-RES-PRIO]

- 1847 • a functional sufficiency assessment of the SHPSFs resource prioritization in case of non-availability induced
1848 by DOS, to fulfil [AVAI-TIME-RES-PRIO]

1849 based on the default configuration required by clause [5.1.2](#).

1850 **Assessment preparation:**

1851 The following documentation for the SHPSF shall be complete:

- 1852 • description how the status of the SHPSFs time sensitive functions can be read or deduced
- 1853 • a list of all time sensitive functions of the SHPSF:
- 1854 - for each of these functions:
- 1855 ▪ the time sensitive availability impact class
- 1856 ▪ whether the function needs network connectivity
- 1857 • prioritization policy for the time sensitive functions of the SHPSF in case of CPU, memory or power resource
1858 conflict

1859 The following test setups shall be prepared:

- 1860 • the SHPSF is set up in default configuration
- 1861 • a test setup to:
- 1862 - read or deduced the status of the time sensitive functions from the SHPSF
- 1863 - induce a DOS status on the SHPSF causing increasing demand on processing resources

1864 **Assessment activities:**

1865 The following activities shall be performed:

- 1866 • verify the correctness and completeness of the documentation
- 1867 • conceptually verify the prioritization policy
- 1868 • progressively higher the intensity of requests to induce a DOS status on the SHPSF
- 1869 - record the status of every time sensitive function

1870 **Assignment of verdict:**

1871 The verdict PASS shall be assigned if:

- 1872 • no indication, that the documentation is incorrect or incomplete, are found; and
- 1873 • the prioritization policy is conceptually valid; and
- 1874 • every time sensitive function:
- 1875 - the status of the function is in accordance with the prioritization policy during DOS.

1876 The verdict FAIL shall be assigned otherwise.

1877 **Supporting Evidence:**

- 1878 • descriptions of the performed tests and records of performed tests

1879 **6.1.8.8 Assessment criteria for [AVAI-TIME-IMP-AMP]**

1880 **Assessment objective:**

1881 The assessment covers:

- 1882 • a conceptual assessment of [AVAI-TIME-NET-PRIO]
 - 1883 • a functional sufficiency assessment of the SHPSFs network amplification, to fulfil [AVAI-TIME-NET-PRIO]
- 1884 based on the default configuration required by clause [5.1.2](#).

1885 **Assessment preparation:**

1886 The following documentation for the SHPSF shall be complete:

- 1887 • a list of all function, whose use can impact the availability of other devices, services or networks of the
1888 SHPSF:
 - 1889 - for each of these functions:
 - 1890 ▪ the function, whose use can impact the availability of other devices, services or networks impact
1891 class
 - 1892 ▪ a list of all used interfaces

1893 The following test setups shall be prepared:

- 1894 • the SHPSF is set up in default configuration
- 1895 • a test setup to:
 - 1896 - execute amplification attacks against the SHPSF
 - 1897 - measure the affective amplification of network traffic caused by the SHPSF

1898 **Assessment activities:**

1899 The following activities shall be performed:

- 1900 • verify the correctness and completeness of the documentation
- 1901 • for every function, whose use can impact the availability of other devices, services or networks with
1902 IMP.FH.DSN.Medium or higher:
 - 1903 - progressively increase the intensity of an amplification attack against this function
 - 1904 - measure the affective amplification of network traffic

1905 **Assignment of verdict:**

1906 The verdict PASS shall be assigned if:

- 1907 • no indication, that the documentation is incorrect or incomplete, are found; and
- 1908 • for every function, whose use can impact the availability of other devices, services or networks with
1909 IMP.FH.DSN.Medium or higher:
 - 1910 - the affective amplification of network traffic is not higher than 10

1911 The verdict FAIL shall be assigned otherwise.

1912 **Supporting Evidence:**

- 1913 • descriptions of the performed tests and records of performed tests

1914 **6.1.8.9 Assessment criteria for [AVAI-TIME-DOS-RATE]**

1915 **Assessment objective:**

1916 The assessment covers:

- 1917 • a conceptual assessment of [AVAI-TIME-DOS-RATE]
 - 1918 • a functional sufficiency assessment of the SHPSFs network rate limiting, to fulfil [AVAI-TIME-DOS-RATE]
- 1919 based on the default configuration required by clause [5.1.2](#).

1920 **Assessment preparation:**

1921 The following documentation for the SHPSF shall be complete:

- 1922 • a list of all time sensitive function of the SHPSF:
 - 1923 - for each of these functions:
 - 1924 ▪ the time sensitive availability impact class
 - 1925 ▪ a list of all used interfaces
- 1926 • a list of all machine interface provided by the SHPSF
- 1927 • rate limiting policy for the SHPSF

1928 The following test setups shall be prepared:

- 1929 • the SHPSF is set up in default configuration
- 1930 • a test setup to:
 - 1931 - induce a DOS status on the SHPSF causing increasing demand on processing resources
 - 1932 - check the status of all time sensitive function with IMP.AVAI.TIME.High

1933 **Assessment activities:**

1934 The following activities shall be performed:

- 1935 • verify the correctness and completeness of the documentation
- 1936 • progressively higher the intensity of requests to induce a DOS status on the SHPSF
 - 1937 - record the status of every time sensitive function with IMP.AVAI.TIME.High

1938 **Assignment of verdict:**

1939 The verdict PASS shall be assigned if:

- 1940 • no indication, that the documentation is incorrect or incomplete, are found; and
- 1941 • the rate limiting policy is conceptually valid; and
- 1942 • for every time sensitive function with IMP.AVAI.TIME.High or higher:
 - 1943 - the status of the function is in accordance with the rate limiting policy during DOS.

1944 The verdict FAIL shall be assigned otherwise.

1945 **Supporting Evidence:**

- 1946 • descriptions of the performed tests and records of performed tests

1947 **6.1.8.10 Assessment criteria for [AVAI-SUM-SCHEDULE]**

1948 **Assessment objective:**

1949 The assessment covers:

- 1950 • a conceptual assessment of [AVAI-SUM-SCHEDULE]
- 1951 • a functional sufficiency assessment of the SHPSFs notification in case of non-availability induced by DOS, to
1952 fulfil [AVAI-TIME-PREV-NOT]

1953 based on the default configuration required by clause [5.1.2](#).

1954 **Assessment preparation:**

1955 The following documentation for the SHPSF shall be complete:

- 1956 • a list of all time sensitive functions of the SHPSF:
- 1957 - for each of these functions:
- 1958 ▪ the time sensitive availability impact class
- 1959 • a list of all software update mechanisms of the SHPSF:
- 1960 - for each of these mechanisms:
- 1961 ▪ whether this mechanism can effect at least one time sensitive function with
1962 IMP.AVAI.TIME.Medium or higher
- 1963 ▪ description how the software update mechanism can be configured

1964 The following test setups shall be prepared:

- 1965 • the SHPSF is set up in default configuration

1966 **Assessment activities:**

1967 The following activities shall be performed:

- 1968 • verify the correctness and completeness of the documentation
- 1969 • for every software update mechanism that can effect at least one time sensitive function with
1970 IMP.AVAI.TIME.Medium or higher:
- 1971 - check whether the application of software updates can be scheduled
- 1972 - record the results

1973 **Assignment of verdict:**

1974 The verdict PASS shall be assigned if:

- 1975 • no indication, that the documentation is incorrect or incomplete, are found; and
- 1976 • for every software update mechanism that can effect at least one time sensitive function with
1977 IMP.AVAI.TIME.Medium or higher:
- 1978 - the application of software updates can be scheduled

1979 The verdict FAIL shall be assigned otherwise.

1980 **Supporting Evidence:**

- 1981 • descriptions of the performed tests and records of performed tests

1982 **6.1.9 Impact minimization**

1983 **6.1.10 Limit attack surface**

1984 **6.1.10.1 Assessment criteria for [LAS-SBOOT]**

1985 **Assessment objective:**

1986 The assessment covers:

- 1987 • a conceptual assessment of [LAS-SBOOT]
- 1988 • a functional sufficiency assessment of the bootloader function used by the SHPSF to fulfil [LAS-SBOOT]

1989 based on the default configuration required by clause [5.1.2](#).

1990 **Assessment preparation:**

1991 The following documentation for the SHPSF shall be complete:

- 1992 • SBOM of the SHPSF's hardware architectural component including information on which software's integrity
1993 and authenticity is protected by the bootloader function
- 1994 • documentation on how the bootloader function verifies the integrity and authenticity of the hardware
1995 architectural component's software

1996 The following test setup shall be prepared:

- 1997 • a test setup for installing integrity and authenticity tampered core software, including a software package
1998 including the tampered core software; or
- 1999 • a test setup for tampering the integrity of installed core software;

2000 **Assessment activities:**

- 2001 • The SHPSF's conformity to [LAS-SBOOT] shall be validated based on the documentation.
- 2002 • The correct implementation of the bootloader function's integrity and authenticity verification of core software
2003 shall be verified based on:
 - 2004 - tampering the integrity and authenticity of installed core software or installing integrity and authenticity
2005 tampered core software; and
 - 2006 - restarting the SHPSF's hardware architectural component

2007 **NOTE:** Typical results are:

- 2008 • the bootloader function refuses to execute the tampered core software (and thus does not execute application
2009 software), and
- 2010 • either halts, resets, or boots into a secure fallback and
- 2011 • an error indication is provided (e.g. via a log, an error code, an LED pattern, etc.).

2012 **Assignment of verdict:**

2013 The verdict PASS shall be assigned if:

- 2014 • the documentation indicates the SHPSF's conformity to [LAS-SBOOT]; and
- 2015 • the SHPSF's hardware architectural component does not execute the modified core software.

2016 Otherwise, the verdict FAIL shall be assigned.

2017 **Supporting Evidence:**

- 2018 • records of the validation of the documentation
- 2019 • descriptions of the performed tests and documentation of associated test records that verify the correct
- 2020 implementation of the bootloader function's integrity and authenticity verification

2021 6.1.11 Logging and monitoring mechanisms

2022 6.1.11.1 Assessment criteria for [LOG-LOW]

2023 **Assessment objective:**

2024 The assessment covers:

- 2025 • a conceptual assessment of [LOG-LOW]
 - 2026 • a functional sufficiency assessment of logging mechanisms used by the SHPSF to fulfil [LOG-LOW]
- 2027 based on the default configuration required by clause [5.1.2](#).

2028 **Assessment preparation:**

2029 The following documentation for the SHPSF shall be complete:

- 2030 • list of all logging mechanisms
- 2031 • documentation on how the logging mechanisms creates logging data
- 2032 • documentation for which events logging data are created by which logging mechanism
- 2033 • documentation on where logging data are stored

2034 The following test setups shall be prepared:

- 2035 • a test user with the necessary permissions has been set up to trigger the events
- 2036 • logging mechanism are enabled on the SHPSF such that at least all the events in the following point are
- 2037 covered
- 2038 • a test setup for triggering the following events: - change of configuration affecting core software;
- 2039 • starts, shutdowns or other changes of operational states of core software;
- 2040 • errors of the core software

2041 **Assessment activities:**

2042 The following activities shall be performed:

- 2043 • Verify whether the *list of all logging mechanisms* is complete
- 2044 • trigger the events listed in *Assessment preparation*
- 2045 - for each event triggered: verify that logging data is created according to the documentation

2046 **Assignment of verdict:**

2047 The verdict PASS shall be assigned if:

- 2048 • the *list of all logging mechanisms* is complete; and
- 2049 • for each event listed in *Assessment preparation* that could be triggered, logging data is created

2050 The verdict FAIL shall be assigned otherwise.

2051 **Supporting Evidence:**

- descriptions of the performed tests and records of performed tests

2053 6.1.11.2 Assessment criteria for [LOG-MEDIUM]

2054 **Assessment objective:**

2055 The assessment covers:

- a conceptual assessment of [LOG-MEDIUM]
- a functional sufficiency assessment of logging mechanisms used by the SHPSF to fulfil [LOG-MEDIUM] based on the default configuration required by clause [5.1.2](#).

2059 **Assessment preparation:**

2060 The following documentation for the SHPSF shall be complete:

- list of all logging mechanisms
- documentation on how the logging mechanisms creates logging data
- documentation for which events logging data are created by which logging mechanism
- documentation on where logging data are stored

2065 The following test setups shall be prepared:

- a test user with the necessary permissions has been set up to trigger the events
- a test setup for triggering the following events: - unsuccessful authentication attempt;
- change of configuration affecting core software;
- starts, shutdowns or other changes of operational states of core software;
- errors of the core software;
- unsuccessful attempt of an identity to gain additional privileges;
- unsuccessful attempt of an identity to access a data asset or function asset

2073 **Assessment activities:**

2074 The following activities shall be performed:

- Verify whether the *list of all logging mechanisms* is complete
- trigger the events listed in *Assessment preparation*
 - for each event triggered: verify that logging data is created according to the documentation

2078 **Assignment of verdict:**

2079 The verdict PASS shall be assigned if:

- the *list of all logging mechanisms* is complete; and
- for each event listed in *Assessment preparation* that could be triggered, logging data is created

2082 The verdict FAIL shall be assigned otherwise.

2083 **Supporting Evidence:**

- descriptions of the performed tests and records of performed tests

2085 **6.1.11.3 Assessment criteria for [LOG-HIGH]**

2086 **Assessment objective:**

2087 The assessment covers:

- 2088 • a conceptual assessment of [LOG-HIGH]
 - 2089 • a functional sufficiency assessment of logging mechanisms used by the SHPSF to fulfil [LOG-HIGH]
- 2090 based on the default configuration required by clause [5.1.2](#).

2091 **Assessment preparation:**

2092 The following documentation for the SHPSF shall be complete:

- 2093 • list of all logging mechanisms
- 2094 • documentation on how the logging mechanisms creates logging data
- 2095 • documentation for which events logging data are created by which logging mechanism
- 2096 • documentation on where logging data are stored

2097 The following test setups shall be prepared:

- 2098 • a test user with the necessary permissions has been set up to trigger the events
- 2099 • a test setup for triggering the following events: - every authentication attempt;
- 2100 • change of configuration affecting core software;
- 2101 • starts, shutdowns or other changes of operational states of core software;
- 2102 • change of configuration affecting application software whom realize function, whose use can cause harm of
- 2103 impact class high;
- 2104 • starts, shutdowns or other changes of operational states of application software whom realize function, whose
- 2105 use can cause harm of impact class high;
- 2106 • errors of the core software;
- 2107 • errors of the application software whom realize function, whose use can cause harm of impact class high;
- 2108 • every attempt of an identity to gain additional privileges;
- 2109 • every attempt of an identity to access a data asset or function asset

2110 **Assessment activities:**

2111 The following activities shall be performed:

- 2112 • Verify whether the *list of all logging mechanisms* is complete
- 2113 • trigger the events listed in *Assessment preparation*
- 2114 - for each event triggered: verify that logging data is created according to the documentation

2115 **Assignment of verdict:**

2116 The verdict PASS shall be assigned if:

- 2117 • the *list of all logging mechanisms* is complete; and
- 2118 • for each event listed in *Assessment preparation* that could be triggered, logging data is created

2119 The verdict FAIL shall be assigned otherwise.

2120 **Supporting Evidence:**

- 2121 • descriptions of the performed tests and records of performed tests

2122 **6.1.11.4 Assessment criteria for [LOG-TIME]**

2123 **Assessment objective:**

2124 The assessment covers:

- 2125 • a functional sufficiency assessment of logging mechanisms used by the SHPSF to fulfil [LOG-TIME]

2126 based on the default configuration required by clause [5.1.2](#).

2127 **Assessment preparation:**

2128 The following documentation for the SHPSF shall be complete:

- 2129 • documentation on how the logging mechanisms creates logging data
- 2130 • documentation for which events logging data are created by which logging mechanism
- 2131 • documentation on where logging data are stored
- 2132 • documentation on the time sources and formats used by logging mechanism

2133 The following test setups shall be prepared:

- 2134 • a test user with the necessary permissions has been set up to trigger the events
- 2135 • logging mechanism are enabled on the SHPSF such that at least all the events in the following point are
2136 covered
- 2137 • a test setup for triggering events as described in *Assessment preparation* in clause [6.1.11.1](#) or clause [6.1.11.2](#)

2138 **Assessment activities:**

2139 The following activities shall be performed:

- 2140 • trigger the events listed in *Assessment preparation* and note the order and approximate time
- 2141 - for each event triggered: verify that the logging data contains a timestamp
- 2142 • for all events triggered: verify that the order and relative times, in which the events where triggered, is
2143 represented by the logging data

2144 **Assignment of verdict:**

2145 The verdict PASS shall be assigned if:

- 2146 • the *list of all logging mechanisms* is complete; and
- 2147 • for each event listed in *Assessment preparation* that could be triggered, the logging data includes a timestamp;
2148 and
- 2149 • the order and relative times, in which the events where triggered, is represented by the logging data

2150 The verdict FAIL shall be assigned otherwise.

2151 **Supporting Evidence:**

- 2152 • descriptions of the performed tests and records of performed tests

2153 6.1.11.5 Assessment criteria for [LOG-TIME-HIGH]

2154 **Assessment objective:**

2155 The assessment covers:

- 2156 • a conceptual assessment of [LOG-TIME-HIGH]
 - 2157 • a functional sufficiency assessment of logging mechanisms used by the SHPSF to fulfil [LOG-TIME-HIGH]
- 2158 based on the default configuration required by clause [5.1.2](#).

2159 **Assessment preparation:**

2160 The following documentation for the SHPSF shall be complete:

- 2161 • documentation on how the logging mechanisms creates logging data
- 2162 • documentation for which events logging data are created by which logging mechanism
- 2163 • documentation on where logging data are stored
- 2164 • documentation on the time sources and formats used by logging mechanism

2165 The following test setups shall be prepared:

- 2166 • a test user with the necessary permissions has been set up to trigger the events
- 2167 • logging mechanism are enabled on the SHPSF such that at least all the events in the following point are
2168 covered
- 2169 • a test setup for triggering events as described in *Assessment preparation* in clause [6.1.11.3](#)

2170 **Assessment activities:**

2171 The following activities shall be performed:

- 2172 • Verify whether the documented time sources are able to produce real time data
- 2173 • trigger the events listed in *Assessment preparation* and note the time
- 2174 - for each event triggered: verify that the logging data contains a timestamp which represents the time, the
2175 event was triggered

2176 **Assignment of verdict:**

2177 The verdict PASS shall be assigned if:

- 2178 • the *list of all logging mechanisms* is complete; and
- 2179 • for each event listed in *Assessment preparation* that could be triggered, the logging data includes a timestamp
2180 which represents the time, the event was triggered

2181 The verdict FAIL shall be assigned otherwise.

2182 **Supporting Evidence:**

- 2183 • descriptions of the performed tests and records of performed tests

2184 6.1.11.6 Assessment criteria for [LOG-STORAGE]

2185 **Assessment objective:**

2186 The assessment covers:

- 2187 • a functional sufficiency assessment of integrity protecting secure storage mechanisms used by the SHPSF to
2188 fulfil [LOG-STORAGE]

2189 based on the default configuration required by clause [5.1.2](#).

2190 **Assessment preparation:**

2191 The following documentation for the SHPSF shall be complete:

- 2192 • documentation on how the logging mechanisms creates logging data
- 2193 • documentation for which events logging data are created by which logging mechanism
- 2194 • documentation on where logging data are stored
- 2195 • documentation on which integrity protecting secure storage mechanism are used to store logging data

2196 The following test setups shall be prepared:

- 2197 • a test user with the necessary permissions has been set up to trigger the events
- 2198 • logging mechanism are enabled on the SHPSF such that at least all the events in the following point are
2199 covered
- 2200 • a test setup for triggering events as described in *Assessment preparation* in clause [6.1.11.2](#) or clause [6.1.11.3](#)
- 2201 • a test setup to safely restart the SHPSF

2202 **Assessment activities:**

2203 The following activities shall be performed:

- 2204 • trigger the events listed in *Assessment preparation*
- 2205 • restart the SHPSF
- 2206 • verify whether all logging data of the triggered events are still present

2207 **Assignment of verdict:**

2208 The verdict PASS shall be assigned if:

- 2209 • for each event listed in *Assessment preparation* that could be triggered, the logging data is still present after
2210 the SHPSF was restarted

2211 The verdict FAIL shall be assigned otherwise.

2212 **Supporting Evidence:**

- 2213 • descriptions of the performed tests and records of performed tests

2214 **6.1.11.7 Assessment criteria for [LOG-BACKUP]**

2215 **Assessment objective:**

2216 The assessment covers:

- 2217 • a conceptual assessment of [LOG-BACKUP]
- 2218 • a functional sufficiency assessment of data backup mechanisms used by the SHPSF to fulfil [LOG-BACKUP]

2219 based on the default configuration required by clause [5.1.2](#).

2220 **Assessment preparation:**

2221 The following documentation for the SHPSF shall be complete:

- 2222 • documentation on how the logging mechanisms creates logging data
- 2223 • documentation for which events logging data are created by which logging mechanism
- 2224 • documentation on where logging data are stored
- 2225 • documentation on which data backup mechanism are used to backup logging data
- 2226 • documentation on logging data packed up destinations
- 2227 The following test setups shall be prepared:
- 2228 • a test user with the necessary permissions has been set up to trigger the events
- 2229 • logging mechanism are enabled on the SHPSF such that at least all the events in the following point are
2230 covered
- 2231 • a test setup for triggering events as described in *Assessment preparation* in clause [6.1.11.3](#)
- 2232 • a test setup to access all documented logging data backup destinations
- 2233 **Assessment activities:**
- 2234 The following activities shall be performed:
- 2235 • verify whether the documentation names data backup mechanisms for logging data of all events described in
2236 *Assessment preparation*
- 2237 • verify whether the documented destinations, where logging data are packed up to, can store these persistently
- 2238 • trigger the events listed in *Assessment preparation*
- 2239 • wait for the automatic backup cycle for the data backup mechanism used to backup logging data
- 2240 • verify whether all logging data of the triggered events are present on the backup destinations
- 2241 **Assignment of verdict:**
- 2242 The verdict PASS shall be assigned if:
- 2243 • all logging data of events described in *Assessment preparation* have at least one data backup mechanism
2244 documented; and
- 2245 • all documented destinations, where logging data are packed up to, can store these persistently; and
- 2246 • all logging data of the triggered events are present on the backup destinations
- 2247 The verdict FAIL shall be assigned otherwise.
- 2248 **Supporting Evidence:**
- 2249 • descriptions of the performed tests and records of performed tests
- 2250 **6.1.12 Deletion mechanisms**
- 2251 **6.1.12.1 Assessment criteria for [DLM-PERM]**
- 2252 **Assessment objective:**
- 2253 The assessment covers:
- 2254 • a conceptual assessment of [DLM-PERM],
- 2255 • a functional completeness assessment on the SHPSF's capabilities that are addressed by [DLM-PERM], and

- 2256 • a functional sufficiency assessment of each deletion mechanism used by the SHPSF to fulfil [DLM-PERM]
 2257 based on the default configuration required by clause [5.1.2](#).

2258 **Assessment preparation:**

2259 The following documentation for the SHPSF shall be complete:

- 2260 • a description of each deletion mechanism, including
- 2261 - deletion scope (i.e. describing what can be deleted by this mechanism),
 - 2262 - method of deletion (e.g. overwriting, access control, changing pointer address, ...),
 - 2263 - method of user interaction and initiation steps,
 - 2264 - whether confirmation is provided after deletion is performed,
 - 2265 - multi-user handling (describing the user rights to delete other users' data)

2266 The following test setups shall be prepared:

- 2267 • a test setup that allows to identify deletion mechanisms on a sample SHPSF in default configuration;
- 2268 • for each deletion mechanism, a test setup that allows to:
 - 2269 - create representative user-related data and install applications,
 - 2270 - access the storage location where data and applications are stored, and
 - 2271 - see the user interaction steps (e.g. menu, dialog, confirmation after deletion)

2272 **Assessment activities:**

2273 The following activities shall be performed:

- 2274 • The SHPSF's conformity to [DLM-PERM] shall be validated based on the documentation.
- 2275 • The correctness and completeness of the documentation shall be verified by checking that all documented
 2276 deletion mechanisms are implemented.
 - 2277 - For each deletion mechanism, its correct implementation shall be verified by:
 - 2278 - generating user-related data and installing an application as a user,
 - 2279 - deleting the generated user-related data and the application and
 - 2280 - checking whether the
 - 2281 ▪ user-related data and the application are permanently removed, e.g. by at least checking the storage
 2282 location of the user-related data and application before and after deletion,
 - 2283 ▪ deletion mechanism is easy to use with limited technical knowledge,
 - 2284 ▪ user can only delete its own data in multi-user systems, and
 - 2285 ▪ user is provided with clear confirmation of deletion after user-related data or a user-installed
 2286 application have been deleted.
 - 2287 • Over all deletion mechanisms, it is to be checked whether all generated sample user-related data and installed
 2288 applications can be permanently removed.

2289 **Assignment of verdict:**

2290 The verdict PASS shall be assigned if:

- 2291 • the documentation indicates the SHPSF's conformity with [DLM-PERM], and

- 2292 • the verification of the correctness and completeness of the documentation was successful, and
- 2293 • the verification of the correct implementation of each deletion mechanism was successful, and
- 2294 • all deletion mechanisms are able to permanently remove all generated user-related data and user-installed
- 2295 applications.

2296 The verdict FAIL shall be assigned otherwise.

2297 **Supporting Evidence:**

- 2298 • records of the validation of the documentation
- 2299 • descriptions of the performed tests and records of performed tests to verify the correctness and completeness
- 2300 of the documentation
- 2301 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each
- 2302 update mechanism and the ability of the SHPSF to delete all generated user-related data and applications

2303 6.1.13 Other product's technical requirements specifications

2304 6.1.13.1 Assessment criteria for [USERNOT-SECREL]

2305 **Assessment objective:**

2306 The assessment covers:

- 2307 • a conceptual assessment of [USERNOT-SECREL];
- 2308 • a functional sufficiency assessment concerning [USERNOT-SECREL] for each user notification mechanism.

2309 **Assessment preparation:**

2310 The following documentation for the SHPSF shall be complete:

- 2311 • a list of all used user notification mechanisms that can provide security-related notifications; and
- 2312 • for each used user notification mechanism that can provide security-related notifications, a description on:
 - 2313 - how it ensures that it uses a language that can be easily understood by users; and
 - 2314 - how it distinguishes the representation of security-related notifications from other notifications.

2315 The following test setups shall be prepared:

- 2316 • for each of the SHPSF's used user notification mechanism that can provide security-related notifications a test
- 2317 setup for:
 - 2318 - generating security-related notifications; and
 - 2319 - (where other notifications are possible) generating other notifications.

2320 **Assessment activities:**

2321 The SHPSF's conformity to [USERNOT-SECREL] shall be validated based on the documentation. The correctness of

2322 the implementation shall be verified by inspecting for each used user notification mechanism for security-related

2323 notifications whether:

- 2324 • one security-related notification is clear, understandable, intelligible, legible and can be easily understood by
- 2325 users; and
- 2326 • (where other notifications are possible), the representation of security-related notifications is clearly
- 2327 distinguished from other notifications.

2328 **Assignment of verdict:**

2329 The verdict PASS shall be assigned if:

- 2330 • the documentation indicates the SHPSF's conformity to [USERNOT-SECRET]; and
- 2331 • the verification of the correct implementation of each used user notification mechanism for security-related
- 2332 notifications was successful.

2333 The verdict FAIL shall be assigned otherwise.

2334 **Supporting Evidence:**

- 2335 • records of the validation of the documentation
- 2336 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each
- 2337 used user notification mechanism for security-related notifications

2338 **6.1.13.2 Assessment criteria for [GUI-SECCONF]**

2339 **Assessment objective:**

2340 The assessment covers:

- 2341 • a conceptual assessment of [GUI-SECCONF];
- 2342 • a functional sufficiency assessment concerning [GUI-SECCONF] for each SHPSF's GUI for security-related
- 2343 configuration functionality.

2344 **Assessment preparation:**

2345 The following documentation for the SHPSF shall be complete:

- 2346 • a list of GUIs for security-related configuration functionality; and
- 2347 • for each GUI for security-related configuration functionality, a description on:
 - 2348 - how it distinguishes the visual representation of security-related configuration options from other
 - 2349 configuration options; and
 - 2350 - how it ensures that it uses a language for communicating the security-related consequences of changing a
 - 2351 security-related configuration option that can be easily understood by users; and
 - 2352 - how it clearly highlights visually when changes to security-related configuration are made by a user.

2353 The following test setups shall be prepared:

- 2354 • a test setup for accessing each SHPSF's GUI for security-related configuration functionality.

2355 **Assessment activities:**

2356 The SHPSF's conformity to [GUI-SECCONF] shall be validated based on the documentation. The correctness of the
 2357 implementation shall be verified by inspecting for each SHPSF's GUI for security-related configuration functionality
 2358 whether:

- 2359 • the visual representation of security-related configuration options is clearly visual distinguished from other
- 2360 configuration options; and
- 2361 • the consequences of one security-related configuration option is communicated in a clear, understandable,
- 2362 intelligible, legible manner and can be easily understood by users; and
- 2363 • the change of one security-related configuration is clearly highlighted visually.

2364 **Assignment of verdict:**

2365 The verdict PASS shall be assigned if:

- 2366
- the documentation indicates the SHPSF's conformity to [GUI-SECCONF]; and
- 2367
- the verification of the correct implementation of each GUI for security-related configuration functionality was
- 2368
- successful.

2369 The verdict FAIL shall be assigned otherwise.

2370 **Supporting Evidence:**

- 2371
- records of the validation of the documentation
- 2372
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each
- 2373
- GUI for security-related configuration functionality

2374 **6.2 Assessment criteria for vulnerability handling activities**

2375 **related to the product**

2376 The assessment criteria specified in CEN/CLC JT013090:2026 (CEN/CLC prEN 40000-1-3) [1] shall be met for the

2377 SHPSF based on the corresponding specified input and output.

2378

2379 Annex A (informative): Relationship between the present
2380 document and the requirements of EU Regulation
2381 2024/2847

2382 **DRAFT ANNEX A - DO NOT CONSIDER THE CONTENT - See identified gaps in Annex F**

2383 The present document has been prepared under the Commission's Standardisation request M/606 - C(2025)618 [i.3] to
2384 provide one voluntary means of conforming to the requirements of Regulation (EU) No 2024/2847 of the European
2385 Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital
2386 elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber
2387 Resilience Act).

2388 Once the present document is cited in the Official Journal of the European Union under that Regulation, compliance
2389 with the normative clauses of the present document given in table 'A.1' confers, within the limits of the scope of the
2390 present document, a presumption of conformity with the corresponding requirements of that Regulation and associated
2391 EFTA regulations.

2392
2393

**Table 'A.1': Relationship between the present document and the requirements of Regulation (EU)
2024/2847 [i.1]**

Harmonised Standard ETSI EN 304 632					
Requirement				Requirement Conditionality	
No	Description	Requirements of Regulation	Clause(s) of the present document	U/C	Condition

1	The design, development, and production of products with digital elements ensures an appropriate level of cybersecurity based on the risks.	Annex I, Part I, (1)	<p>[ACM-FH] 5.1.3.1 [AUM-FH] 5.1.3.2 [AUTHZ-LP] 5.1.3.3 [AUTHZ-R] 5.1.3.4 [AVAI-TIME-RECO-POW] 5.1.7.1 [AVAI-TIME-NETW] 5.1.7.2 [AVAI-TIME-RECO-NETW] 5.1.7.3 [AVAI-TIME-OUTA-NOT] 5.1.7.4 [AVAI-TIME-PREV-NOT] 5.1.7.5 [AVAI-TIME-NET-PRIO] 5.1.7.6 [AVAI-TIME-RES-PRIO] 5.1.7.7 [AVAI-TIME-IMP-AMP] 5.1.7.8 [AVAI-TIME-DOS-RATE] 5.1.7.9 [AVAI-SUM-SCHEDULE] 5.1.7.10 [CONF-SSM] 5.1.5.1 [CONF-COM] 5.1.5.2 [CRY-SOTA] 5.1.12.4 [CRY-CCK-PRE-LEN] 5.1.12.5 [CRY-CCK-GEN] 5.1.12.6 [CRY-PW-PRE-COM] 5.1.12.7 [CRY-PW-GEN-COM] 5.1.12.8 [CRY-PW-USR-COM] 5.1.12.9 [DLM-PERM] 5.1.11.1 [DMIN-DJST] 5.1.6.1 [GUI-SECCONF] 5.1.12.3 [INT-SWPCK] 5.1.4.1 [INT-COM] 5.1.4.2 [LAS-INVAL] 5.1.9.1 [LAS-INSAN] 5.1.9.2 [LAS-PHY-INF] 5.1.9.3 [LAS-LOGIC-INF] 5.1.9.4 [LAS-APP] 5.1.9.5 [LAS-SBOOT] 5.1.9.6 [LOG-LOW] 5.1.10.1 [LOG-MEDIUM] 5.1.10.2 [LOG-HIGH] 5.1.10.3 [LOG-TIME] 5.1.10.4 [LOG-TIME-HIGH] 5.1.10.5 [LOG-STORAGE] 5.1.10.6 [LOG-BACKUP] 5.1.10.7 [NKEV-MKAV] 5.1.1.1 [NKEV-SUM-SUPPORT] 5.1.1.2 [NKEV-SUM-PROVIDE] 5.1.1.3 [NKEV-SUM-AUTO] 5.1.1.4 [NKEV-SUM-NOTIF] 5.1.1.5 [SDC-AUM-FH] 5.1.2.1 [SDC-SUM-AUTO] 5.1.2.2 [SDC-SUM-NOTIF] 5.1.2.3 [SDC-FRM] 5.1.2.4 [USERNOT-NOSECFUC] 5.1.12.1</p>	U	
---	---	----------------------	---	---	--

Harmonised Standard ETSI EN 304 632					
Requirement				Requirement Conditionality	
No	Description	Requirements of Regulation	Clause(s) of the present document	U/C	Condition
			[USERNOT-SECREL] 5.1.12.2		
2	Products with digital elements are made available on the market without known exploitable vulnerabilities.	Annex I, Part I, (2)(a)	[NKEV-MKAV] 5.1.1.1	U	
3	Products with digital elements are 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.	Annex I, Part I, (2)(b)	[LAS-LOGIC-INF] 5.1.9.4 [LAS-APP] 5.1.9.5 [SDC-AUM-FH] 5.1.2.1 [SDC-SUM-AUTO] 5.1.2.2 [SDC-SUM-NOTIF] 5.1.2.3 [SDC-FRM] 5.1.2.4	U	
4	Products with digital elements 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.	Annex I, Part I, (2)(c)	[NKEV-SUM-SUPPORT] 5.1.1.2 [NKEV-SUM-PROVIDE] 5.1.1.3 [NKEV-SUM-AUTO] 5.1.1.4 [NKEV-SUM-NOTIF] 5.1.1.5 [SDC-SUM-AUTO] 5.1.2.2 [SDC-SUM-NOTIF] 5.1.2.3	U	
5	Products with digital elements ensure protection from Unauthorized access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible Unauthorized access.	Annex I, Part I, (2)(d)	[ACM-FH] 5.1.3.1 [AUM-FH] 5.1.3.2 [AUTHZ-LP] 5.1.3.3 [AUTHZ-R] 5.1.3.4 [LOG-MEDIUM] 5.1.10.2 [LOG-HIGH] 5.1.10.3 [SDC-AUM-FH] 5.1.2.1	U	
6	Products with digital elements 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 state-of-the-art mechanisms, and by using other technical means.	Annex I, Part I, (2)(e)	[CONF-SSM] 5.1.5.1 [CONF-COM] 5.1.5.2	U	
7	Products with digital elements protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorized by the user, and report on corruptions.	Annex I, Part I, (2)(f)	[INT-SWPCK] 5.1.4.1 [INT-COM] 5.1.4.2 [LOG-LOW] 5.1.10.1 [LOG-MEDIUM] 5.1.10.2 [LOG-HIGH] 5.1.10.3	U	

Harmonised Standard ETSI EN 304 632					
Requirement				Requirement Conditionality	
No	Description	Requirements of Regulation	Clause(s) of the present document	U/C	Condition
8	Products with digital elements process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimization).	Annex I, Part I, (2)(g)	[DMIN-DJST] 5.1.6.1	U	
9	Products with digital elements protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks.	Annex I, Part I, (2)(h)	[AVAI-TIME-RECO-POW] 5.1.7.1 [AVAI-TIME-NETW] 5.1.7.2 [AVAI-TIME-RECO-NETW] 5.1.7.3 [AVAI-TIME-OUTA-NOT] 5.1.7.4 [AVAI-TIME-PREV-NOT] 5.1.7.5 [AVAI-TIME-NET-PRIO] 5.1.7.6 [AVAI-TIME-RES-PRIO] 5.1.7.7 [AVAI-TIME-DOS-RATE] 5.1.7.9 [AVAI-SUM-SCHEDULE] 5.1.7.10	U	
10	Products with digital elements minimize the negative impact by the products themselves or connected products on the availability of services provided by other products or networks.	Annex I, Part I, (2)(i)	[AVAI-TIME-IMP-AMP] 5.1.7.8	U	
11	Products with digital elements are designed, developed and produced to limit attack surfaces, including external interfaces.	Annex I, Part I, (2)(j)	[LAS-INVAL] 5.1.9.1 [LAS-INSAN] 5.1.9.2 [LAS-PHY-INF] 5.1.9.3 [LAS-LOGIC-INF] 5.1.9.4 [LAS-APP] 5.1.9.5 [LAS-SBOOT] 5.1.9.6	U	
12	Products with digital elements are designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques.	Annex I, Part I, (2)(k)	[AVAI-TIME-RECO-POW] 5.1.7.1 [AVAI-TIME-NET-PRIO] 5.1.7.6 [AVAI-TIME-RES-PRIO] 5.1.7.7	U	
13	Products with digital elements 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.	Annex I, Part I, (2)(l)	[LOG-LOW] 5.1.10.1 [LOG-MEDIUM] 5.1.10.2 [LOG-HIGH] 5.1.10.3 [LOG-TIME] 5.1.10.4 [LOG-TIME-HIGH] 5.1.10.5 [LOG-STORAGE] 5.1.10.6 [LOG-BACKUP] 5.1.10.7 [NKEV-SUM-NOTIF] 5.1.1.5 [USERNOT-NOSECFUC] 5.1.12.1	U	

Harmonised Standard ETSI EN 304 632					
Requirement					Requirement Conditionality
No	Description	Requirements of Regulation	Clause(s) of the present document	U/C	Condition
14	Products with digital elements 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.	Annex I, Part I, (2)(m)	[DLM-PERM] 5.1.11.1 [SDC-FRM] 5.1.2.4	U	
15	Vulnerability handling requirements	Annex I, Part II	clause 5.2	U	

Key to columns:**Requirement:****No**

A unique identifier for one row of the table which may be used to identify a requirement.

Description

A textual reference to the requirement.

Requirements of Regulation

Identification of article(s) defining the requirement in the Regulation.

Clause(s) of the present document

Identification of clause(s) defining the requirement in the present document unless another document is referenced explicitly.

Requirement Conditionality**U/C**

Indicates whether the requirement is unconditionally applicable (U) or is conditional upon the manufacturer's claimed functionality of the equipment (C).

Condition

Explains the conditions when the requirement is or is not applicable for a requirement which is classified "conditional".

2394 Presumption of conformity stays valid only as long as a reference to the present document is maintained in the list
 2395 published in the Official Journal of the European Union. Users of the present document should consult frequently the
 2396 latest list published in the Official Journal of the European Union.

2397 Other Union legislation may be applicable to the product(s) falling within the scope of the present document.

2398 Annex B (informative): Guidance for the application of the 2399 present document

2400 The following approach can be used (e.g. by manufacturers)

- 2401 • to develop products that are compliant the present document; or
- 2402 • to analyse the compliance of a product to the present document.

2403 The approach is constructed such that it uses parts of an assessment of cybersecurity risks and can be integrated into the
 2404 management of cybersecurity risks.

- 2405 • Step 1 - check if the product is in scope of the present document provided in clause [1](#) by:

2406 - verifying that the product is a SHPSF as specified within the "technical description" of the "category of
 2407 product" number "17." by Regulation (EU) 2025/2392 [i.2]; and

2408 - identifying the product context by:

- 2409 ▪ identifying the product's architectural components; and
- 2410 ▪ identifying all data processed by the product (data assets); and
- 2411 ▪ identifying all functions provided by the product (function assets); and

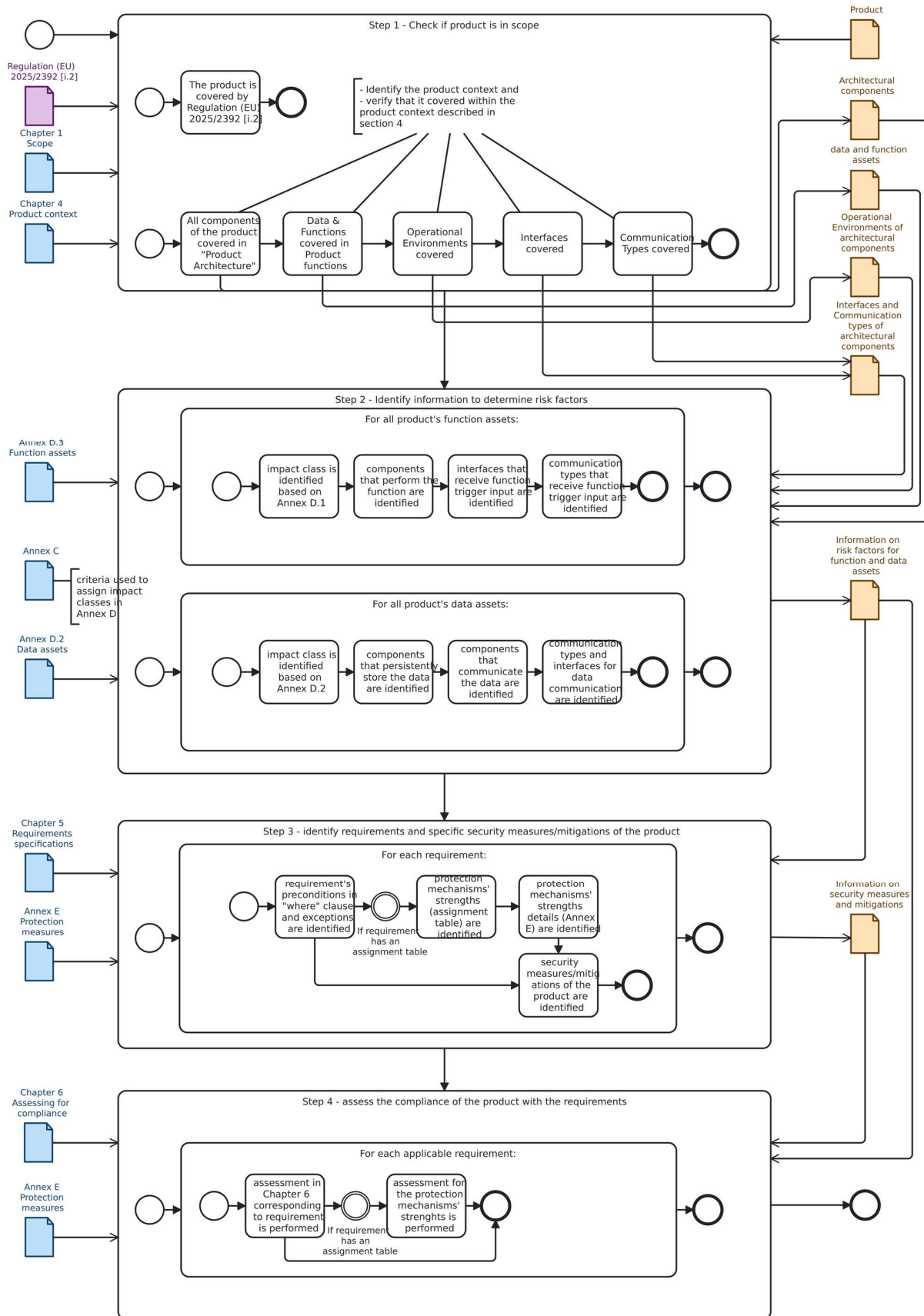
- 2412 ▪ identifying the architectural components' operational environments; and
- 2413 ▪ identifying the architectural components' interfaces and communication types; and
- 2414 - verifying that the product is covered within the product context described in clause 4 by:
- 2415 ▪ verifying that the architectural components of the product are covered within the product
- 2416 architecture described in clause 4.2; and
- 2417 ▪ verifying that the data processed by the product and the functions provided by the product are
- 2418 covered within clause 4.1; and
- 2419 ▪ verifying that the architectural components' operational environments are covered within
- 2420 clause 4.3; and
- 2421 ▪ verifying that the architectural components' interfaces and communication types are covered within
- 2422 clause 4.4.
- 2423 NOTE 1: The identification of the items mentioned above can be reused for assessing the compliance
- 2424 of the product with the requirements in clause 5.
- 2425 NOTE 2: If a product is a SHPSF as specified by Regulation (EU) 2025/2392 [i.2] but is not covered
- 2426 within the product context described in clause 4, it is assumed that the product is not or not
- 2427 completely covered by the present document. In such cases informing ETSI Technical Committee
- 2428 Cyber Working Group for EUSR (CYBER-EUSR) via the [Committee Support Staff](#) might help to
- 2429 address those products in potential revisions of the present document.
- 2430 • Step 2 - identify information to determine risk factors by:
- 2431 - identifying for each function provided by the product:
- 2432 ▪ its impact classes according to clause D.2; and
- 2433 ▪ the architectural components that perform the function; and
- 2434 ▪ the communication types and the interfaces that can receive corresponding function trigger input;
- 2435 and
- 2436 - identifying for each data processed by the product:
- 2437 ▪ its impact classes according to clause D.1
- 2438 ▪ the architectural components that persistently store the data; and
- 2439 ▪ the architectural components that can communicate the data; and
- 2440 ▪ the communication types and the interfaces over which the data is communicated.
- 2441 NOTE 3: If data processed by the product or functions provided by the product are not covered
- 2442 within clause 4.1, clause C.1 can be used to identify impact classes for function and data assets that
- 2443 are outside the scope of the present document.
- 2444 • Step 3 - identify concrete requirements for and specific security measures/mitigations of the product that
- 2445 satisfy those requirements by:
- 2446 - for each requirement in clause 5:
- 2447 ▪ identifying the requirements applicability by evaluating the requirement's potential preconditions
- 2448 and exceptions based on the product's properties; and
- 2449 ▪ (for requirements that include assignment tables) identifying the required protection mechanisms'
- 2450 strengths (specified in annex E) by evaluating the requirement's assignment table based on the
- 2451 product's properties determining the attack surface and impact parameters; and
- 2452 ▪ identifying the specific security measures/mitigations that satisfy the requirement.

2453 NOTE 4: An assignment table can yield multiple mechanisms' strengths from different
2454 circumstances, which all have to be satisfied.

2455 EXAMPLE: Authentication requirements prior to changes of a SHPSFs configuration are different
2456 whether the changes can be made via a web GUI, accessible from adjacent or public networks, a GUI,
2457 accessible from the SHPSFs touchscreen, or a console, accessible be connecting to a serial port. All of
2458 these cases can be simultaneously present on the same SHPSF.

- 2459 • Step 4 - assess the compliance of the product with the requirements in clause [5](#) by:
 - 2460 - for each requirement in clause [5](#), performing the corresponding assessment for compliance described in
2461 clause [6](#) (the functional sufficiency assessments for different protection measures strengths are specified
2462 in annex [E](#)) by:
 - 2463 ▪ preparing the assessment for the product; and
 - 2464 ▪ performing the assessment activities for the product; and
 - 2465 ▪ assigning an assessment verdict for the product; and
 - 2466 ▪ generating the supporting evidences for the assessment.

2467 The figure [B.1](#) provides a graphical representation of the guidance for the application of the present document.



2469 **Figure B.1: Graphical representation on guidance for the application of the present document**

2470 **Annex C (informative): Information on the methodology for**
 2471 **the assessment of cybersecurity risks used to develop the**
 2472 **present document**

2473 **This informative annex is intended to provide information on the methodology for the assessment of**
 2474 **cybersecurity risks used to develop the present document.**

2475 C.1 Guidance for determining impact classes

2476 C.1.1 General

2477 The present document uses the following criteria to determine the impact classes of different specific SHPSF assets
 2478 provided in annex [D](#).

2479 C.1.2 confidential data

2480 **confidentiality impact class low (IMP.CONF.Low):**

2481 The disclosure may lead to:

- 2482 • inconvenient consequences on the user(s); or
- 2483 • additional or increased attack opportunities over a short time and limited to communication types not higher
 2484 than local on the SHPSF.

2485 **confidentiality impact class medium (IMP.CONF.Medium):**

2486 The disclosure may lead to:

- 2487 • serious impact on the user(s);
- 2488 • additional or increased attack opportunities over a short time on the SHPSF or a limited number of other
 2489 products; or
- 2490 • additional or increased attack opportunities over a prolonged time limited to non-key-functionalities on the
 2491 SHPSF.

2492 **confidentiality impact class high (IMP.CONF.High):**

2493 The disclosure may lead to:

- 2494 • significant or even irreversible impact on the user(s) (e.g. personal or financial harm);
- 2495 • additional or increased attack opportunities over a prolonged time on the SHPSF or a limited number of other
 2496 products; or
- 2497 • additional or increased attack opportunities over a short time on a significant number of other products.

2498 C.1.3 loss sensitive data

2499 **loss sensitive availability impact class low (IMP.AVALLOSS.Low):**

2500 The loss may lead to:

- 2501 • inconvenient consequences on the user(s); or
- 2502 • non-availability of non-key-functionalities on the SHPSF for a short time.

2503 **loss sensitive availability impact class medium (IMP.AVALLOSS.Medium):**

2504 The loss may lead to:

- 2505 • serious impact on the user(s); or
- 2506 • non-availability of key-functionalities of the SHPSF over a short time; or
- 2507 • non-availability of non-key-functionalities on the SHPSF for a prolonged time.

2508 **loss sensitive availability impact class high (IMP.AVALOSS.High):**

2509 The loss may lead to:

- 2510 • significant or even irreversible impact on the user(s) (e.g. personal or financial harm);
- 2511 • non-availability of key-functionalities of the SHPSF for a prolonged time; or
- 2512 • permanent non-availability of non-key-functionalities of the SHPSF

2513 C.1.4 time sensitive data and time sensitive function

2514 **time sensitive availability impact class low (IMP.AVAL.TIME.Low):**

2515 The delay of availability may lead to:

- 2516 • non-availability of non-key-functionalities on the SHPSF for a short time.

2517 **time sensitive availability impact class medium (IMP.AVAL.TIME.Medium):**

2518 The delay of availability may lead to:

- 2519 • non-availability of key-functionalities on the SHPSF for a short time; or
- 2520 • non-availability of non-key-functionalities on the SHPSF for a prolonged time.

2521 **time sensitive availability impact class high (IMP.AVAL.TIME.High):**

2522 The delay of availability may lead to:

- 2523 • non-availability of key-functionalities of the SHPSF for a prolonged time; or
- 2524 • permanent non-availability of non-key-functionalities of the SHPSF.

2525 C.1.5 integrity relevant data and integrity relevant function

2526 **integrity impact class low (IMP.INT.Low):**

2527 The tampering may lead to:

- 2528 • inconvenient consequences on the user(s);
- 2529 • additional or increased attack opportunities for a short time and limited to communication types not higher
2530 than local on the SHPSF; or
- 2531 • non-availability of non-key-functionalities on the SHPSF for a short time.

2532 **integrity impact class medium (IMP.INT.Medium):**

2533 The tampering may lead to:

- 2534 • serious impact on the user(s);
- 2535 • additional or increased attack opportunities over a short time on the SHPSF or a limited number of other
2536 products;

2537 • additional or increased attack opportunities over a prolonged time limited to non-key-functionalities on the
2538 SHPSF; or

2539 • non-availability of key-functionalities on the SHPSF for a short time; or

2540 • non-availability of non-key-functionalities on the SHPSF for a prolonged time.

2541 **integrity impact class high (IMP.INT.High):**

2542 The tampering may lead to:

2543 • significant or even irreversible impact on the user(s) (e.g. personal or financial harm);

2544 • additional or increased attack opportunities for a prolonged time on the SHPSF or a limited number of other
2545 products;

2546 • additional or increased attack opportunities for a short time on a significant number of other products;

2547 • non-availability of key-functionalities of the SHPSF for a prolonged time; or

2548 • permanent non-availability of non-key-functionalities of the SHPSF

2549 Annex D (normative): Relationship between specific data
2550 and functions assets covered by the present document to
2551 impact classes for generic asset categories

2552 D.1 Data assets

2553 **Table D.1: Mapping of specific data assets to impact classes for generic data asset categories**

specific data asset	impact class for data asset categories			
	impact class for confidential SHPSF data	impact class for integrity relevant SHPSF data	impact class for time critical availability relevant SHPSF data	impact class for loss critical availability relevant SHPSF data
locking element position data	IMP.CONF.Medium	IMP.INT.Medium	IMP.AVAI.TIME.Medium	IMP.AVAI.LOSS.Medium
battery status data	IMP.CONF.Medium	IMP.INT.Medium	IMP.AVAI.TIME.Low	IMP.AVAI.LOSS.Medium
fire detection data	IMP.CONF.Low	IMP.INT.High	IMP.AVAI.TIME.High	IMP.AVAI.LOSS.Low
inflammable/explosive gas detection data	IMP.CONF.Low	IMP.INT.High	IMP.AVAI.TIME.High	IMP.AVAI.LOSS.Low
window/door opening status data	IMP.CONF.Low	IMP.INT.Medium	IMP.AVAI.TIME.Low	IMP.AVAI.LOSS.Low
intrusion detection data	IMP.CONF.Medium	IMP.INT.Medium	IMP.AVAI.TIME.Medium	IMP.AVAI.LOSS.Low
function fault detection data	IMP.CONF.Medium	IMP.INT.Medium	IMP.AVAI.TIME = Maximum (IMP.AVAI.TIME, IMP.INT of the erroneous function)	IMP.AVAI.LOSS.Low
object tamper detection data	IMP.CONF.Medium	IMP.CONF.Medium	IMP.CONF.Medium	IMP.AVAI.LOSS.Low
human fall detection data	IMP.CONF.Medium	IMP.CONF.Medium	IMP.AVAI.TIME.High	IMP.AVAI.LOSS.Low
audio input data	IMP.CONF.Medium	IMP.INT.Medium	IMP.AVAI.TIME.Low	no
video input data	IMP.CONF.Medium	IMP.INT.Medium	IMP.AVAI.TIME.Low	no
network status data	IMP.CONF.Medium	IMP.INT.Medium	IMP.AVAI.TIME.Medium	IMP.AVAI.LOSS.Low
authorization policy data	IMP.CONF.Medium	IMP.INT.High	IMP.AVAI.TIME.Medium	IMP.AVAI.LOSS.Low
SHPSF state data	IMP.CONF.Medium	IMP.INT.Medium	IMP.AVAI.TIME.Medium	IMP.AVAI.LOSS.Low
logging data	IMP.CONF = IMP.CONF of confidential data contained in the logging data	IMP.INT = Highest IMP.FH	IMP.AVAI.TIME.Low	IMP.AVAI.LOSS.Medium
software package	IMP.CONF = IMP.CONF of confidential data contained in the package	IMP.INT = Highest IMP.INT of SHPSF's integrity relevant function	no	no
cryptographic security parameter	IMP.CONF = Maximum (Maximum (IMP.CONF, IMP.INT of all data assets whose protection relies on the confidentiality of the cryptographic security parameter), Maximum (IMP.INT, IMP.INT, IMP.FH of all function assets whose protection relies on the confidentiality of the cryptographic security parameter))	IMP.INT = Maximum (Maximum (IMP.CONF, IMP.INT of all data assets whose protection relies on the integrity of the cryptographic security parameter), Maximum (IMP.INT, IMP.INT, IMP.FH of all function assets whose protection relies on the integrity of the cryptographic security parameter))	IMP.AVAI.TIME = Maximum (IMP.AVAI.TIME of all data assets whose availability relies on the availability of the cryptographic security parameter)	IMP.AVAI.LOSS = Maximum (IMP.AVAI.LOSS of all data assets which are lost when the cryptographic security parameter is lost)
actuator control data	no	IMP.INT = Maximum IMP.FH of controlled actuator control function	IMP.AVAI.TIME = Maximum IMP.AVAI.TIME of controlled actuator control function	no
function configuration data	IMP.CONF = Maximum IMP.FH of configured function	IMP.INT = Maximum IMP of configured function	IMP.AVAI.TIME = Maximum IMP.AVAI.TIME of configured function	IMP.AVAI.LOSS = Maximum IMP.AVAI.TIME of configured function

2554 D.2 Function assets

2555 Table D.2: Mapping of specific function assets to impact classes for generic function asset
2556 categories

specific function asset	impact class for function asset categories		
	impact class for integrity relevant function	impact class for time sensitive function	impact class for function, whose use can cause harm
SHPSF exterior lock function	IMP.INT.Medium	IMP.AVAI.TIME.Medium	IMP.FH.High
SHPSF interior lock function	IMP.INT.Medium	IMP.AVAI.TIME.Medium	IMP.FH.Medium
SHPSF basic protection object lock function	IMP.INT.Low	IMP.AVAI.TIME.Medium	IMP.FH.Low
SHPSF medium protection object lock function	IMP.INT.Medium	IMP.AVAI.TIME.Medium	IMP.FH.Medium
SHPSF high protection object lock function	IMP.INT.High	IMP.AVAI.TIME.Medium	IMP.FH.High
SHPSF actuator alarm function	IMP.INT.High	IMP.AVAI.TIME.High	IMP.FH.Medium
intrusion and hold up alarm function	IMP.INT.Medium	IMP.AVAI.TIME.Medium	IMP.FH.Medium
social alarm function	IMP.INT.High	IMP.AVAI.TIME.High	IMP.FH.Medium
fire/gas alarm function	IMP.INT.Medium	IMP.AVAI.TIME.Medium	IMP.FH.Medium
positioning function	IMP.INT.Medium	IMP.AVAI.TIME.Medium	no
SHPSF surrounding monitoring function	IMP.INT.Medium	IMP.AVAI.TIME.High	IMP.FH.Medium
SHPSF lock function with failsafe	IMP.INT.Medium	IMP.AVAI.TIME.Low	IMP.FH.High
physical security detection function	IMP.INT.High	IMP.AVAI.TIME.High	IMP.FH.Medium
physical security notification function	IMP.INT.High	IMP.AVAI.TIME.High	IMP.FH.Medium
power supply function	IMP.INT.Medium	IMP.AVAI.TIME = Maximum IMP.AVAI.TIME of functions of controlled hardware architectural component	IMP.FH = Maximum (IMP.FH.SP, IMP.AVAI.TIME) of functions of controlled hardware architectural component; if controlling power of other devices at least IMP.FH.Low
object tamper detection function	IMP.INT.Medium	IMP.INT.Medium	no
audio input function	IMP.INT.Medium	IMP.AVAI.TIME.Low	IMP.FH.Medium
video input function	IMP.INT.Medium	IMP.AVAI.TIME.Low	IMP.FH.Medium
audio output function	IMP.INT.Medium	IMP.AVAI.TIME.Low	IMP.FH.Medium
video output function	IMP.INT.Medium	IMP.AVAI.TIME.Low	IMP.FH.Medium
SHPSF function which can communicate SHPSF data	IMP.INT = Maximum (IMP.CONF, IMP.INT) of communicated data	IMP.AVAI.TIME = IMP.AVAI.TIME of communicated data	IMP.FH = Maximum (IMP.FH.Low, IMP.CONF of communicated data)
connection function	IMP.INT.Low	IMP.AVAI.TIME.Low	IMP.FH.Medium
SHPSF function which can modify SHPSF data	IMP.INT = IMP.INT of modified data	no	IMP.FH = IMP.INT of modified data
data presenting function	IMP.INT = Maximum (IMP.CONF, IMP.INT) of presented data	IMP.AVAI.TIME = Maximum IMP.AVAI.TIME of presented data	IMP.FH = Maximum IMP.CONF of presented data
detection function	IMP.INT = Maximum (IMP.CONF, IMP.INT) of output data or triggered functions	IMP.AVAI.TIME = Maximum IMP.AVAI.TIME of output data or triggered functions	IMP.FH = Maximum IMP.CONF of output data or IMP.FH.SP of triggered functions
sensing function	IMP.INT = Maximum IMP.INT of measured data	IMP.AVAI.TIME = Maximum IMP.AVAI.TIME of measured data	IMP.FH = Maximum IMP.CONF of measured data
actuator control function	IMP.INT = Maximum IMP.FH of controlled function	IMP.AVAI.TIME = Maximum IMP.AVAI.TIME of controlled function	IMP.FH = Maximum IMP.FH of controlled function
SHPSF physical tamper detection function	IMP.INT = Maximum IMP.INT of the hardware architectural component's functions	IMP.AVAI.TIME = Maximum IMP.AVAI.TIME of the hardware architectural component's functions	no

2557 The contents of the column *impact class for function, whose use can cause harm* of table [D.2](#) are split into details in
2558 table [D.3](#).

2559
2560

Table D.3: Mapping of specific function assets to impact classes for different aspects of function, whose use can cause harm

specific function asset	impact class for function asset categories			
	impact class for function, whose use can impact the safety or privacy of human entities	impact class for function, whose use can impact the availability of other devices, services or networks	impact class for function, which can communicate confidential data	impact class for function, which can modify integrity relevant data
SHPSF exterior lock function	IMP.FH.SP.High	no	no	no
SHPSF interior lock function	IMP.FH.SP.Medium	no	no	no
SHPSF basic protection object lock function	IMP.FH.SP.Low	no	no	no
SHPSF medium protection object lock function	IMP.FH.SP.Medium	no	no	no
SHPSF high protection object lock function	IMP.FH.SP.High	no	no	no
SHPSF actuator alarm function	IMP.FH.SP.Medium	no	no	no
intrusion and hold up alarm function	IMP.FH.SP.Medium	no	no	no
social alarm function	IMP.FH.SP.Medium	no	no	no
fire/gas alarm function	IMP.FH.SP.Medium	no	no	no
positioning function	IMP.FH.SP.Medium	no	no	IMP.FH.MINT.Medium
SHPSF surrounding monitoring function	IMP.FH.SP.High	no	IMP.FH.CCON.High	no
SHPSF lock function with failsafe	IMP.FH.SP.High	no	no	no
physical security detection function	IMP.FH.SP.Medium	no	no	no
physical security notification function	IMP.FH.SP.Medium	no	no	no
power supply function	IMP.FH.SP = Maximum IMP.FH.SP of functions of controlled hardware architectural component	IMP.FH.DSN.Low if controlling power of other devices, no otherwise	no	no
object tamper detection function	no	no	no	no
audio input function	IMP.FH.SP.Medium	no	no	no
video input function	IMP.FH.SP.Medium	no	no	no
audio output function	IMP.FH.SP.Medium	no	no	no
video output function	IMP.FH.SP.Medium	no	no	no
SHPSF function which can communicate SHPSF data	no	IMP.FH.DSN.Low	IMP.FH.CCON = IMP.CONF of communicated data	no
connection function	no	IMP.FH.DSN.Medium	no	no
SHPSF function which can modify SHPSF data	no	no	no	IMP.FH.MINT = IMP.INT of modified data
data presenting function	IMP.FH.SP = Maximum IMP.CONF of presented data	no	IMP.FH.CCON = Maximum IMP.CONF of presented data	no
detection function	IMP.FH.SP = Maximum IMP.CONF of output data or IMP.FH.SP of triggered functions	no	no	no
sensing function	IMP.FH.SP = Maximum IMP.CONF of measured data	no	no	IMP.FH.MINT = Maximum IMP.INT of measured data

specific function asset	impact class for function asset categories			
	impact class for function, whose use can impact the safety or privacy of human entities	impact class for function, whose use can impact the availability of other devices, services or networks	impact class for function, which can communicate confidential data	impact class for function, which can modify integrity relevant data
actuator control function	IMP.FH.SP = Maximum IMP.FH.SP of controlled function	IMP.FH.DSN = Maximum IMP.FH.DSN of controlled function	IMP.FH.CCON = Maximum IMP.FH.CCON of controlled function	IMP.FH.MINT = Maximum IMP.FH.MINT of controlled function
SHPSF physical tamper detection function	no	no	no	no

2561 Annex E (normative): Protection measures

2562 E.1 authentication mechanism strength

2563 E.1.1 [AUM-FH] Authentication for functions whose use can cause harm

2564 E.1.1.1 General

2565 The present document specifies the strength of authentication mechanisms by their resistance against certain attack
2566 types. Those attack types are constructed such that mechanisms of higher strength protect against all attack types
2567 required for lower strengths.

2568 E.1.1.2 authentication - strength level basic

2569 The authentication - strength level basic shall protect against the following attack types:

2570 **limited presentation attack:** Opportunistic presentation attacks on authentication mechanisms based on authentication
2571 factors of the type inherence, using authentication factors of another entity

2572 **limited brute force attack:** Opportunistic guessing attacks on authentication mechanisms based on authentication
2573 factors of the type knowledge, by guessing manually without the use of technical aids.

2574 E.1.1.3 authentication - strength level normal

2575 The authentication - strength level normal shall protect against the following attack types:

2576 **automated brute force attack:** Brute force attacks on authentication mechanisms based on authentication factors of the
2577 type knowledge, by systematic try out with technical.

2578 **presentation attack:** Presentation attacks on authentication mechanisms based on authentication factors of the type
2579 inherence, using medium effort methods like e.g. photos, cut out masks, audio replays, video replays, AI generated
2580 voices

2581 **automated security token spoofing attack:** Security token spoofing attacks on authentication mechanisms based on
2582 authentication factors of the type possession, by using authentication factors sourced from other uses or self-created,
2583 without using any specific knowledge of the targeted authentication mechanisms.

2584 **replay attack:** An attacker intercepts valid data transmissions and retransmits them to mimic the original
2585 communication partner for accepting an authentication based on the authentication factors of the type knowledge or
2586 possession (e.g. a session token).

2587 **person in the middle attack:** An attacker secretly intercepts and alters the authentication between two parties who
2588 believe they are communicating directly with each other based on the authentication factors of the type knowledge or
2589 possession (e.g. a session token).

2590 E.1.1.4 authentication - strength level enhanced

2591 The authentication - strength level enhanced shall protect against the following attack types:

2592 **targeted presentation attack:** Presentation attacks on authentication mechanisms based on authentication factors of the
2593 type inherence, using enhanced effort methods like e.g. (partial) silicone masks, layered prints

2594 **targeted brute force attack:** Brute force attacks on authentication mechanisms based on authentication factors of the
2595 type knowledge, by systematic try out with technical aids, making use of target specific information.

2596 **targeted security token spoofing attack:** Security token spoofing attacks on authentication mechanisms based on
2597 authentication factors of the type possession, by using authentication factors sourced from devices of the same type as
2598 the SHPSF or self-created, using specific knowledge of the targeted authentication mechanisms and the SHPSF.

2599 **replay attack:** An attacker intercepts valid data transmissions and retransmits them to mimic the original
2600 communication partner for accepting an authentication based on the authentication factors of the type knowledge or
2601 possession (e.g. a session token).

2602 **person in the middle attack:** An attacker secretly intercepts and alters the authentication between two parties who
2603 believe they are communicating directly with each other based on the authentication factors of the type knowledge or
2604 possession (e.g. a session token).

2605 E.1.1.5 authentication - strength level strong

2606 The authentication - strength level strong shall protect against the following attack types:

2607 **elaborate presentation attack:** Presentation attacks on authentication mechanisms based on authentication factors of
2608 the type inherence", using high effort methods like e.g. highly realistic silicone or latex masks, limb replicas, trained
2609 deepfakes

2610 **elaborate brute force attack:** Brute force attacks on authentication mechanisms based on authentication factors of the
2611 type knowledge, by systematic try out with technical aids, making use of target specific information, and unrestricted
2612 duration.

2613 **elaborate security token spoofing attack:** Security token spoofing attacks on authentication mechanisms based on
2614 authentication factors of the type possession, by using authentication factors created or sourced from devices of the
2615 same type as the SHPSF and modified, specifically for the targeted authentication mechanisms.

2616 **replay attack:** An attacker intercepts valid data transmissions and retransmits them to mimic the original
2617 communication partner for accepting an authentication based on the authentication factors of the type knowledge or
2618 possession (e.g. a session token).

2619 **person in the middle attack:** An attacker secretly intercepts and alters the authentication between two parties who
2620 believe they are communicating directly with each other based on the authentication factors of the type knowledge or
2621 possession (e.g. a session token).

2622 E.1.2 Assessment for authentication mechanism strength

2623 E.1.2.1 Assessment criteria regarding the protection against limited presentation 2624 attacks

2625 **Assessment objective:**

2626 The assessment covers functional testing of authentication mechanisms that provide a basic level of protection and use
2627 authentication factors of the type inherence against limited presentation attacks.

2628 **Assessment preparation:**

- 2629 • the SHPSF shall be set up in default configuration
- 2630 • a genuine enrolled biometric template in the corresponding authentication mechanism with credential for
2631 authentication shall be created
- 2632 • at least one interface, where the authentication mechanism is reachable shall be documented

2633 **Assessment activities:**

- 2634 • authentication at the created genuine enrolled biometric template shall be attempted using the correct genuine
- 2635 enrolled biometric template identifier, if present, and authentication factors, not belonging to the person who
- 2636 set up the account, for at least five times or ten minutes at highest archivable query frequency
- 2637 • the outcome and used authentication factor of each attempt shall be recorded

2638 **Assignment of verdict:**

2639 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts.

2640 The verdict FAIL shall be assigned otherwise.

2641 **Supporting Evidence:**

- 2642 • description of the performed test
- 2643 • all test records of the performed test

2644 E.1.2.2 Assessment criteria regarding the protection against targeted presentation

2645 attacks

2646 **Assessment objective:**

2647 The assessment covers functional testing of authentication mechanisms that provide a enhanced level of protection and

2648 use authentication factors of the type inherence against targeted presentation attacks.

2649 **Assessment preparation:**

- 2650 • the SHPSF shall be set up in default configuration
- 2651 • a genuine enrolled biometric template in the corresponding authentication mechanism with credential for
- 2652 authentication shall be created
- 2653 • at least one interface, where the authentication mechanism is reachable shall be documented
- 2654 • authentication factors shall be fabricated using common materials and tools as well as readily available source
- 2655 materials. The fabrication process shall not be longer than *one workday* per authentication factor.

2656 **Assessment activities:**

- 2657 • authentication at the created genuine enrolled biometric template shall be attempted using the correct genuine
- 2658 enrolled biometric template identifier, if present, and at least two fabricated authentication factors tried at least
- 2659 five times with slightly different parameters each
- 2660 • the outcome and used authentication factor of each attempt shall be recorded

2661 **Assignment of verdict:**

2662 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts.

2663 The verdict FAIL shall be assigned otherwise.

2664 **Supporting Evidence:**

- 2665 • description of the performed test
- 2666 • all test records of the performed test

2667 E.1.2.3 Assessment criteria regarding the protection against elaborate presentation

2668 attacks

2669 **Assessment objective:**

2670 The assessment covers functional testing of authentication mechanisms that provide a high level of protection and use
2671 authentication factors of the type inherence against elaborate presentation attacks.

2672 **Assessment preparation:**

- 2673 • the SHPSF shall be set up in default configuration
- 2674 • a genuine enrolled biometric template in the corresponding authentication mechanism with credential for
2675 authentication shall be created
- 2676 • at least one interface, where the authentication mechanism is reachable shall be documented
- 2677 • authentication factors shall be fabricated using specialized materials and tools as well as cumbersome
2678 extracted source materials. The duration of the fabrication process per authentication factor is not restricted.

2679 **Assessment activities:**

- 2680 • authentication at the created genuine enrolled biometric template shall be attempted using the correct genuine
2681 enrolled biometric template identifier, if present, and at least two fabricated authentication factors tried at least
2682 five times with slightly different parameters each
- 2683 • the outcome and used authentication factor of each attempt shall be recorded

2684 **Assignment of verdict:**

2685 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts.

2686 The verdict FAIL shall be assigned otherwise.

2687 **Supporting Evidence:**

- 2688 • description of the performed test
- 2689 • all test records of the performed test

2690 **E.1.2.4 Assessment criteria regarding the protection against limited brute force**
2691 **attacks**

2692 **Assessment objective:**

2693 The assessment covers functional testing of authentication mechanisms that provide a basic level of protection and use
2694 authentication factors of the type knowledge against limited brute force attacks.

2695 **Assessment preparation:**

- 2696 • the SHPSF shall be set up in default configuration
- 2697 • at least one interface, where the authentication mechanism is reachable shall be documented

2698 the security insurance time (T_{SI}) for this assessment is 10 minutes (600s)

2699 **Assessment activities:**

2700 the minimal recommended complexity of passwords accepted by the mechanism ($C_{PW,min}$) shall be determined;
2701 e.g. $C_{PW,min} = (10)^6$ for a 6-digit PIN or $C_{PW,min} = \frac{9!}{(9-5)!}$ for a pattern of 5 nonrecurring nodes in a field of 9 notes

2702 the maximum sustained login attempt frequency ($f_{LA,max}$) shall be determined; e.g. $f_{LA,max} = \frac{5}{5 \cdot 35 + 3600s}$ for 3 seconds
2703 per login attempt + a one-hour waiting period after 5 failed login attempts

2704 the probability of guessing a completely random password of the minimal recommended complexity (p_{GRP}) shall be
2705 calculated by $p_{GRP} = T_{SI} * f_{LA,max} / C_{PW,min}$

- 2706 • the methods and outcome of each step shall be recorded

2707 **Assignment of verdict:**

2708 The verdict PASS shall be assigned if the calculated probability p_{GRP} is less than 10^{-2} .

2709 The verdict FAIL shall be assigned otherwise.

2710 **Supporting Evidence:**

2711 • the authentication mechanism and the interface via which it was accessed

2712 • all test records of the performed test

2713 **E.1.2.5 Assessment criteria regarding the protection against targeted brute force**
2714 **attacks**

2715 **Assessment objective:**

2716 The assessment covers functional testing of authentication mechanisms that provide an enhanced level of protection and
2717 use authentication factors of the type knowledge against targeted brute force attacks.

2718 **Assessment preparation:**

2719 • the SHPSF shall be set up in default configuration

2720 • at least one interface, where the authentication mechanism is reachable shall be documented

2721 the security insurance time (T_{SI}) for this assessment one month ($2,6 * 10^6s$)

2722 **Assessment activities:**

2723 the minimal recommended complexity of passwords accepted by the mechanism ($C_{PW,min}$) shall be determined; e.g.,
2724 $C_{PW,min} = (26 * 2 + 10)^8$ for minimum 8 characters of upper-case or lower-case letters or numbers

2725 the maximum sustained login attempt frequency ($f_{LA,max}$) shall be determined; e.g. $f_{LA,max} = (0,1s)^{-1}$ for 10 login
2726 attempt per second

2727 the probability of guessing a completely random password of the minimal recommended complexity (p_{GRP}) shall be
2728 calculated by $p_{GRP} = T_{SI} * f_{LA,max} / C_{PW,min}$

2729 • the methods and outcome of each step shall be recorded

2730 **Assignment of verdict:**

2731 The verdict PASS shall be assigned if the calculated probability p_{GRP} is less than 10^{-6} .

2732 The verdict FAIL shall be assigned otherwise.

2733 **Supporting Evidence:**

2734 • the authentication mechanism and the interface via which it was accessed

2735 • all test records of the performed test

2736 **E.1.2.6 Assessment criteria regarding the protection against automated brute force**
2737 **attacks**

2738 **Assessment objective:**

2739 The assessment covers functional testing of authentication mechanisms that provide a medium level of protection and
2740 use authentication factors of the type knowledge against targeted brute force attacks.

2741 **Assessment preparation:**

2742 • the SHPSF shall be set up in default configuration

- 2743 • at least one interface, where the authentication mechanism is reachable shall be documented
- 2744 the security insurance time (T_{SI}) for this assessment is one day (86400s)
- 2745 **Assessment activities:**
- 2746 the minimal recommended complexity of passwords accepted by the mechanism ($C_{PW,min}$) shall be determined;
- 2747 e.g. $C_{PW,min} = (26 * 2 + 10)^8$ for minimum 8 characters of upper-case case or lower-case letters or numbers
- 2748 the maximum sustained login attempt frequency ($f_{LA,max}$) shall be determined; e.g. $f_{LA,max} = \frac{5}{5*3s+3600s}$ for 3 seconds
- 2749 per login attempt + a one-hour waiting period after 5 failed login attempts
- 2750 the probability of guessing a completely random password of the minimal recommended complexity (p_{GRP}) shall be
- 2751 calculated by $p_{GRP} = T_{SI} * f_{LA,max} / C_{PW,min}$

- 2752 • the methods and outcome of each step shall be recorded

2753 **Assignment of verdict:**

2754 The verdict PASS shall be assigned if the calculated probability p_{GRP} is less than 10^{-6} .

2755 The verdict FAIL shall be assigned otherwise.

2756 **Supporting Evidence:**

- 2757 • the authentication mechanism and the interface via which it was accessed
- 2758 • all test records of the performed test

2759 **E.1.2.7 Assessment criteria regarding the protection against presentation attacks**

2760 **Assessment objective:**

2761 The assessment covers functional testing of authentication mechanisms that provide a medium level of protection and

2762 use authentication factors of the type inherence against presentation attacks.

2763 **Assessment preparation:**

- 2764 • the SHPSF shall be set up in default configuration
- 2765 • a genuine enrolled biometric template in the corresponding authentication mechanism with credential for
- 2766 authentication shall be created
- 2767 • at least one interface, where the authentication mechanism is reachable shall be documented
- 2768 • authentication factors shall be fabricated using readily available materials and tools as well as readily available
- 2769 source materials. The fabrication process shall not be longer than *twenty* minutes per authentication factor.

2770 NOTE: Readily available source materials are e.g. fingerprints on everyday items or publicly available photos.

2771 Readily available materials and tools are of adhesive tape, printer paper, common printers.

2772 **Assessment activities:**

- 2773 • authentication at the created account shall be attempted using the correct account name, if present, and at least
- 2774 two fabricated authentication factors tried at least five times with slightly different parameters each
- 2775 • the outcome and used fabricated authentication factor of each attempt shall be recorded

2776 **Assignment of verdict:**

2777 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts.

2778 The verdict FAIL shall be assigned otherwise.

2779 **Supporting Evidence:**

- 2780 • description of the performed test
- 2781 • all test records of the performed test

2782 E.1.2.8 Assessment criteria regarding the protection against elaborate brute force 2783 attacks

2784 **Assessment objective:**

2785 The assessment covers functional testing of authentication mechanisms that provide a high level of protection and use
2786 authentication factors of the type knowledge against targeted brute force attacks.

2787 **Assessment preparation:**

- 2788 • the SHPSF shall be set up in default configuration
- 2789 • at least one interface, where the authentication mechanism is reachable shall be documented

2790 the security insurance time (T_{SI}) for this assessment is five years ($1,6 * 10^8s$)

2791 **Assessment activities:**

2792 the minimal recommended complexity of passwords accepted by the mechanism ($C_{PW,min}$) shall be determined;
2793 e.g. $(26 * 2 + 10)^8$ for minimum 8 characters of upper-case case or lower-case letters or numbers

2794 the maximum sustained login attempt frequency ($f_{LA,max}$) shall be determined; e.g. $(0,1s)^{-1}$ for 10 login attempt per
2795 second

2796 the probability of guessing a completely random password of the minimal recommended complexity (p_{GRP}) shall be
2797 calculated by $p_{GRP} = T_{SI} * f_{LA,max} / C_{PW,min}$

- 2798 • the methods and outcome of each step shall be recorded

2799 **Assignment of verdict:**

2800 The verdict PASS shall be assigned if the calculated probability is less than 10^{-6} .

2801 The verdict FAIL shall be assigned otherwise.

2802 **Supporting Evidence:**

- 2803 • the authentication mechanism and the interface via which it was accessed
- 2804 • all test records of the performed test

2805 E.1.2.9 Assessment criteria regarding the protection against automated security 2806 token spoofing attacks

2807 **Assessment objective:**

2808 The assessment covers functional testing of authentication mechanisms that provide a medium level of protection and
2809 use authentication factors of the type possession against automated security token spoofing attacks.

2810 **Assessment preparation:**

- 2811 • the SHPSF shall be set up in default configuration
- 2812 • an account in the corresponding authentication mechanism with a security token for authentication shall be
2813 created
- 2814 • at least one interface, where the authentication mechanism is reachable shall be documented
- 2815 • security tokens, that match specifications of the interfaces, via which the authentication mechanism is
2816 reachable, shall be prepared or created without using any specific knowledge of the authentication mechanism

2817 **Assessment activities:**

2818 • authentication at the created account shall be attempted using the correct account name, if present, and the
2819 prepared or created security tokens

2820 • the outcome and used authentication factor of each attempt shall be recorded

2821 **Assignment of verdict:**

2822 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts, except where the used
2823 authentication factor exactly matches the configured one.

2824 The verdict FAIL shall be assigned otherwise.

2825 **Supporting Evidence:**

2826 • description of the performed test

2827 • all test records of the performed test

2828 **E.1.2.10 Assessment criteria regarding the protection against targeted security token**
2829 **spoofing attacks**

2830 **Assessment objective:**

2831 The assessment covers functional testing of authentication mechanisms that provide an enhanced level of protection and
2832 use authentication factors of the type possession against targeted security token spoofing attacks.

2833 **Assessment preparation:**

2834 • the SHPSF shall be set up in default configuration

2835 • an account in the corresponding authentication mechanism with a security token for authentication shall be
2836 created

2837 • at least one interface, where the authentication mechanism is reachable shall be documented

2838 • security tokens, shall be prepared or created, which match the specifications of the authentication mechanism.

2839 **Assessment activities:**

2840 • authentication at the created account shall be attempted using the correct account name, if present, and the
2841 prepared or created security tokens

2842 • the outcome and used authentication factor of each attempt shall be recorded

2843 **Assignment of verdict:**

2844 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts, except where the used
2845 authentication factor exactly matches the configured one.

2846 The verdict FAIL shall be assigned otherwise.

2847 **Supporting Evidence:**

2848 • description of the performed test

2849 • all test records of the performed test

2850 **E.1.2.11 Assessment criteria regarding the protection against elaborate security token**
2851 **spoofing attacks**

2852 **Assessment objective:**

2853 The assessment covers functional testing of authentication mechanisms that provide a high level of protection and use
2854 authentication factors of the type possession against elaborate security token spoofing attacks.

2855 **Assessment preparation:**

- 2856 • the SHPSF shall be set up in default configuration
- 2857 • an account in the corresponding authentication mechanism with a security token for authentication shall be
2858 created
- 2859 • at least one interface, where the authentication mechanism is reachable shall be documented
- 2860 • security tokens, shall be prepared or created, which match the specifications of the authentication mechanism
2861 and use information extracted from the original security token.

2862 **Assessment activities:**

- 2863 • authentication at the created account shall be attempted using the correct account name, if present, and the
2864 prepared or created security tokens
- 2865 • the outcome and used authentication factor of each attempt shall be recorded

2866 **Assignment of verdict:**

2867 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts, except where the used
2868 authentication factor exactly matches the configured one.

2869 The verdict FAIL shall be assigned otherwise.

2870 **Supporting Evidence:**

- 2871 • description of the performed test
- 2872 • all test records of the performed test

2873 **E.1.2.12 Assessment criteria regarding the protection against replay attacks**

2874 **Assessment objective:**

2875 The assessment covers functional testing of authentication mechanisms that use authentication factors of the type
2876 knowledge or possession (e.g. a session token) against replay attacks.

2877 **Assessment preparation:**

- 2878 • the SHPSF shall be set up in default configuration
- 2879 • the authentication mechanism shall be active
- 2880 • a communication partner with active authentication mechanisms shall be set up for the SHPSF
- 2881 • a capture and replay tool between SHPSF and its communication partner shall be set up
- 2882 • at least one interface, where the authentication mechanism is reachable shall be documented

2883 **Assessment activities:**

- 2884 • Initiate a connection between the SHPSF and its communication partner.
- 2885 • Use a capture tool to record the transmitted message or transaction data.
- 2886 • Replay (retransmit) the captured message to the product using a suitable tool in place to mimic the original
2887 communication partner.
- 2888 • Record if the product accepts the retransmitted data

2889 **Assignment of verdict:**

2890 The verdict PASS shall be assigned if it is not possible to impersonate as the communication partner.

2891 The verdict FAIL shall be assigned otherwise.

2892 **Supporting Evidence:**

- 2893 • description of the performed test
- 2894 • all test records of the performed test

2895 **E.1.2.13 Assessment criteria regarding the protection against PitM attacks**

2896 **Assessment objective:**

2897 The assessment covers functional testing of authentication mechanisms that use authentication factors of the type
2898 knowledge or possession (e.g. a session token) against PitM attacks.

2899 **Assessment preparation:**

- 2900 • the SHPSF shall be set up in default configuration
- 2901 • the authentication mechanism shall be active
- 2902 • a communication partner with active authentication mechanisms shall be set up for the SHPSF
- 2903 • a capture and PitM tool between SHPSF and its communication partner shall be set up
- 2904 • at least one interface, where the authentication mechanism is reachable shall be documented

2905 **Assessment activities:**

- 2906 • Initiate a connection between the SHPSF and its communication partner.
- 2907 • Attempt to capture data (user credentials, tokens, etc.) with the tool in place and actively intercept
2908 communication to impersonate the communication partner during:
 - 2909 - generation and communication of authentication factors for the communication partner (if not
2910 pre-configured); and
 - 2911 - authentication of the communication partner
- 2912 • Record if the impersonation as communication partner is successful

2913 **Assignment of verdict:**

2914 The verdict PASS shall be assigned if it is not possible to impersonate as the communication partner.

2915 The verdict FAIL shall be assigned otherwise.

2916 **Supporting Evidence:**

- 2917 • description of the performed test
- 2918 • all test records of the performed test

2919 E.2 integrity protection strength

2920 E.2.1 [INT-SWPCK] Software package verification

2921 E.2.1.1 General

2922 The present document specifies software package verification mechanisms' strength, by certain protection measures.
2923 Those measures are constructed such that measures of higher strength typically have less attack vectors than lower
2924 strength measures.

2925 E.2.1.2 software package integrity verification - strength level basic

2926 Mechanisms for the software package integrity verification - strength level basic shall:

- 2927 • explicitly obtain the confirmation of an authorized entity that the integrity and authenticity of a software
2928 package has been verified by the entity, where the software package's source is determined by the entity; or
- 2929 • explicitly obtain the confirmation of an authorized entity that the authenticity of a software package has been
2930 verified by the entity and use a hash or checksum provided by the entity for the software package to verify its
2931 integrity, where the software package's source is determined by the entity.

2932 E.2.1.3 software package integrity verification - strength level normal

2933 Mechanisms for the software package integrity verification - strength level normal shall ensure that a software package
2934 has been obtained from a trusted source over a secure communication channel that meets INT.COM.Enhanced.

2935 E.2.1.4 software package integrity verification - strength level enhanced

2936 Mechanisms for the software package integrity verification - strength level enhanced shall verify the authenticity and
2937 integrity of a software package using cryptographic digital signature verification.

2938 E.2.2 [INT-COM] Communication of integrity relevant data

2939 E.2.2.1 General

2940 The present document specifies the strength of mechanisms to protect the integrity of communicated integrity relevant
2941 data by their resistance against certain attack types. Those attack types are constructed such that mechanisms of higher
2942 strength protect against all attack types required for lower strengths.

2943 E.2.2.2 communication of integrity relevant data - protection strength level basic

2944 The communication of integrity relevant data - protection strength level basic shall protect against the following attack
2945 types:

2946 **accidental bit flip:** Accidental change of data by natural causes.

2947 E.2.2.3 communication of integrity relevant data - protection strength level normal

2948 The communication of integrity relevant data - protection strength level normal shall protect against the following
2949 attack types:

2950 **replay attack:** An attacker intercepts valid transmissions and then retransmits those captured messages to the same
2951 interface to deceive it into performing unauthorized actions.

2952 **accidental bit flip:** Accidental change of data by natural causes.

2953 **direct identity spoofing attack:** An attacker mimics another entity to gain a trust relationship with the SHPSF

2954 **downgrade of communication protocols attack:** An attacker forces to use of a legacy, less secure, communication
2955 protocol

2956 E.2.2.4 communication of integrity relevant data - protection strength level enhanced

2957 The communication of integrity relevant data - protection strength level enhanced shall protect against the following
2958 attack types:

2959 **replay attack:** An attacker intercepts valid transmissions and then retransmits those captured messages to the same
2960 interface to deceive it into performing unauthorized actions.

2961 **person in the middle attack:** An attacker secretly alters the communication between the SHPSF and another entity or
2962 another part of the SHPSF to gain a trusted relationship with the involved communication partners without their
2963 knowledge.

2964 **accidental bit flip:** Accidental change of data by natural causes.

2965 **direct identity spoofing attack:** An attacker mimics another entity to gain a trust relationship with the SHPSF

2966 **downgrade of communication protocols attack:** An attacker forces to use of a legacy, less secure, communication
2967 protocol

2968 E.2.2.5 communication of integrity relevant data - protection strength level strong

2969 The communication of integrity relevant data - protection strength level strong shall protect against the following attack
2970 types:

2971 **replay attack:** An attacker intercepts valid transmissions and then retransmits those captured messages to the same
2972 interface to deceive it into performing unauthorized actions.

2973 **person in the middle attack:** An attacker secretly alters the communication between the SHPSF and another entity or
2974 another part of the SHPSF to gain a trusted relationship with the involved communication partners without their
2975 knowledge.

2976 **accidental bit flip:** Accidental change of data by natural causes.

2977 **direct identity spoofing attack:** An attacker mimics another entity to gain a trust relationship with the SHPSF

2978 **downgrade of communication protocols attack:** An attacker forces to use of a legacy, less secure, communication
2979 protocol

2980 E.3 confidentiality protection strength

2981 E.3.1 [CONF-SSM] Confidentiality protecting persistent storage for 2982 confidential data

2983 E.3.1.1 General

2984 The present document specifies confidentiality protecting secure storage mechanisms' strength, by certain security
2985 properties. Those properties are constructed such that mechanisms of higher strength have the properties of lower
2986 strength mechanisms.

2987 E.3.1.2 confidential persistent storage - strength level basic

2988 Mechanisms for the confidential persistent storage - strength level basic shall encrypt such that decryption is only
2989 possible for the SHPSF.

2990 E.3.1.3 confidential persistent storage - strength level normal

2991 Mechanisms for the confidential persistent storage - strength level normal shall encrypt such that decryption is

- 2992 • only possible for the SHPSF and
- 2993 • only performed after a successful authentication.

2994 E.3.1.4 confidential persistent storage - strength level enhanced

2995 Mechanisms for the confidential persistent storage - strength level enhanced shall encrypt supported by hardware, such
2996 that

2997 • decryption is only possible for the SHPSF after a successful authentication and

2998 • the extraction of the encryption key is prevented by hardware.

2999 E.3.1.5 confidential persistent storage - strength level strong

3000 Mechanisms for the confidential persistent storage - strength level strong shall prevent the extraction of data by
3001 hardware.

3002 E.3.2 [CONF-COM] Communication of confidential data

3003 E.3.2.1 General

3004 The present document specifies the strength of mechanisms to protect the confidentiality of communicated confidential
3005 data by their resistance against certain attack types. Those attack types are constructed such that mechanisms of higher
3006 strength protect against all attack types required for lower strengths.

3007 E.3.2.2 authentication - strength level strong

3008 The authentication - strength level strong shall protect against the following attack types:

3009 **eavesdropping**: An attacker secretly intercepts the communication between the SHPSF and another entity or another
3010 part of the SHPSF.

3011 E.3.2.3 communication of confidential data - protection strength level normal

3012 The communication of confidential data - protection strength level normal shall protect against the following attack
3013 types:

3014 **eavesdropping**: An attacker secretly intercepts the communication between the SHPSF and another entity or another
3015 part of the SHPSF.

3016 **direct identity spoofing attack**: An attacker mimics another entity to gain a trust relationship with the SHPSF

3017 **downgrade of communication protocols attack**: An attacker forces to use of a legacy, less secure, communication
3018 protocol

3019 E.3.2.4 communication of confidential data - protection strength level enhanced

3020 The communication of confidential data - protection strength level enhanced shall protect against the following attack
3021 types:

3022 **eavesdropping**: An attacker secretly intercepts the communication between the SHPSF and another entity or another
3023 part of the SHPSF.

3024 **person in the middle attack**: An attacker secretly alters the communication between the SHPSF and another entity or
3025 another part of the SHPSF to gain a trusted relationship with the involved communication partners without their
3026 knowledge.

3027 **direct identity spoofing attack**: An attacker mimics another entity to gain a trust relationship with the SHPSF

3028 **downgrade of communication protocols attack**: An attacker forces to use of a legacy, less secure, communication
3029 protocol

3030 E.3.2.5 communication of confidential data - protection strength level strong

3031 The communication of confidential data - protection strength level strong shall protect against the following attack
3032 types:

3033 **eavesdropping**: An attacker secretly intercepts the communication between the SHPSF and another entity or another
3034 part of the SHPSF.

3035 **person in the middle attack**: An attacker secretly alters the communication between the SHPSF and another entity or
3036 another part of the SHPSF to gain a trusted relationship with the involved communication partners without their
3037 knowledge.

3038 **direct identity spoofing attack**: An attacker mimics another entity to gain a trust relationship with the SHPSF

3039 **downgrade of communication protocols attack**: An attacker forces to use of a legacy, less secure, communication
3040 protocol

3041 **Annex F (informative): Relationship between the present**
3042 **document and the covered/not covered cybersecurity risks**

3043 **This informative annex is intended to provide the relevant information on the covered/not covered cybersecurity**
3044 **risks and still under discussion.**

3045 **The information provided in the column "Risk coverage" is based on a preliminary analysis which is planned to**
3046 **be expanded in the future and still under discussion.**

3047

Table 'F.1': Covered threats and remaining risks acceptance

No.	Threat Actor	Threat action	Asset	Threat details		Requirement(s) for mitigation	Relevant attack surface parameter	Risk coverage
[1]	A threat actor	(mis)uses	a function whose use can cause harm	on the SHPSF		Prevention: [ACM-FH] 5.1.3.1 [AUM-FH] 5.1.3.2 [AUTHZ-LP] 5.1.3.3 [AUTHZ-R] 5.1.3.4 [AVAI-TIME-IMP-AMP] 5.1.7.8 [LAS-PHY-INF] 5.1.9.3 [LAS-LOGIC-INF] 5.1.9.4 [LAS-APP] 5.1.9.5 [SDC-AUM-FH] 5.1.2.1 Information: [LOG-LOW] 5.1.10.1 [LOG-MEDIUM] 5.1.10.2 [LOG-HIGH] 5.1.10.3 [LOG-TIME] 5.1.10.4 [LOG-TIME-HIGH] 5.1.10.5 [LOG-STORAGE] 5.1.10.6 [LOG-BACKUP] 5.1.10.7 [USERNOT-NOSECFUC] 5.1.12.1 Restoration: [SDC-FRM] 5.1.2.4	COM, IF and POE	C
[2]	A threat actor	tamper s	integrity relevant data	permanently stored on the SHPSF				N
[3]	A threat actor	tamper s	integrity relevant data	volatile stored on the SHPSF				N
[4]	A threat actor	tamper s	integrity relevant data	communicated from or to the architectural component		Prevention: [INT-COM] 5.1.4.2	COM, IF and POE	C
[5]	A threat actor	discloses	confidential data	on the SHPSF	unnecessarily processed	Prevention: [DMIN-DJST] 5.1.6.1		C
[6]	A threat actor	discloses	confidential data	permanently stored on the SHPSF	during storage	Prevention: [CONF-SSM] 5.1.5.1	POE	C
[7]	A threat actor	discloses	confidential data	permanently stored on the SHPSF	after deletion	Prevention: [DLM-PERM] 5.1.11.1		N
[8]	A threat actor	discloses	confidential data	volatile stored on the SHPSF	during usage			N
[9]	A threat actor	discloses	confidential data	volatile stored on the SHPSF	after usage			N
[10]	A threat actor	discloses	confidential data	communicated from or to the architectural component		Prevention: [CONF-COM] 5.1.5.2	COM, IF and POE	C
[11]	A threat actor	tamper s	loss sensitive data	permanently stored on the SHPSF	during storage			N
[12]	A threat actor	tamper s	integrity relevant function	on the SHPSF		Prevention: [INT-SWPCK] 5.1.4.1 [LAS-SBOOT] 5.1.9.6		N

No.	Threat Actor	Threat action	Asset	Threat details		Requirement(s) for mitigation	Relevant attack surface parameter	Risk coverage
[13]	A threat actor	impacts the availability of	time sensitive function	on the SHPSF	by interruption caused by a software update installation	Prevention: [AVAI-SUM-SCHEDULE] 5.1.7.10		C
[14]	A threat actor	impacts the availability of	time sensitive function	on the SHPSF	by interruption of power supply	Information: [AVAI-TIME-OUTA-NOT] 5.1.7.4 [AVAI-TIME-PREV-NOT] 5.1.7.5 Restoration: [AVAI-TIME-RECO-POW] 5.1.7.1		C
[15]	A threat actor	impacts the availability of	time sensitive function	on the SHPSF	by interruption of network connection	Prevention: [AVAI-TIME-NETW] 5.1.7.2 Information: [AVAI-TIME-OUTA-NOT] 5.1.7.4 [AVAI-TIME-PREV-NOT] 5.1.7.5 Restoration: [AVAI-TIME-RECO-NETW] 5.1.7.3		C
[16]	A threat actor	impacts the availability of	time sensitive function	on the SHPSF	due to overloading of a resource or connection	Prevention: [AVAI-TIME-NET-PRIO] 5.1.7.6 [AVAI-TIME-RES-PRIO] 5.1.7.7 [AVAI-TIME-DOS-RATE] 5.1.7.9 Information: [AVAI-TIME-OUTA-NOT] 5.1.7.4	IF	C
[17]	A threat actor	exploits an implementation vulnerability to compromise	a product cybersecurity asset			Prevention: [LAS-INVAL] 5.1.9.1 [LAS-INSAN] 5.1.9.2 [NKEV-MKAV] 5.1.1.1 Information: [NKEV-SUM-NOTIF] 5.1.1.5 [SDC-SUM-NOTIF] 5.1.2.3 Restoration: [NKEV-SUM-SUPPORT] 5.1.1.2 [NKEV-SUM-PROVIDE] 5.1.1.3 [NKEV-SUM-AUTO] 5.1.1.4 [SDC-SUM-AUTO] 5.1.2.2		C
[18]	A user	unconsciously performs incorrect actions		on the SHPSF		Prevention: [GUI-SECCONF] 5.1.12.3 Information: [GUI-SECCONF] 5.1.12.3	IF.Human	C
[19]	A user	performs insecure actions		on the SHPSF	because the user is not aware of security relevant information	Prevention: [USERNOT-SECREL] 5.1.12.2 Information: [USERNOT-SECREL] 5.1.12.2	IF.Human	C

No.	Threat Actor	Threat action	Asset	Threat details	Requirement(s) for mitigation	Relevant attack surface parameter	Risk coverage
[20]	A user	unknowingly creates confidential	audio or video capture data	on the SHPSF		IF.Human	C

- 3048
- 3049
- The columns *Threat Actor*, *Threat Action*, *Asset*, and *Threat Details* describe the threat scenario under consideration.
- 3050
- 3051
- The column *Requirement(s) for mitigation* refers to the mitigations of the risks that arise from the threat scenario.
- 3052
- 3053
- The *Relevant attack surface parameter* column describes which of the attack surface parameters make a difference in mitigation.
- 3054
- 3055
- The *Risk coverage* column describes whether the risk associated with the threat scenario has been reduced to an acceptable residual risk (C) or not (N).

3056 **Annex G (informative): Relationship between the present**

3057 **document and ETSI EN 303 645/ ETSI TS 103 701**

3058 **This informative annex is intended to provide a mapping between the present document and the content of ETSI**

3059 **TC CYBER's existing work on CIoT devices (ETSI EN 303 645/ ETSI TS 103 701).**