



Cyber Security (CYBER); Cyber Resilience Act (CRA); Cybersecurity requirements for smart home general purpose virtual assistants

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-0011 >

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.....		15
13	4 Product context.....		17
14	4.1 Product functions		17
15	4.1.1 Virtual assistant functions		17
16	4.1.2 Supporting functions		18
17	4.1.3 Data assets.....		18
18	4.2 Product Architecture.....		19
19	4.3 Operational Environment.....		20
20	4.4 Interfaces.....		20
21	4.5 Distribution of security functions		21
22	4.6 Users		21
23	4.7 Use cases.....		21
24	4.7.1 General		21
25	4.7.2 Use case profiles		21
26	4.8 Security Profiles.....		22
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.....		24
31	5.1.1.2 [NKEV-SUM-SUPPORT] Secure software update mechanism.....		24
32	5.1.1.3 [NKEV-SUM-PROVIDE] Secure software update mechanism for core components		24
33	5.1.1.4 [NKEV-SUM-AUTO] Automated security updates.....		24
34	5.1.1.5 [NKEV-SUM-NOTIF] Update notifications		24
35	5.1.2 Default configuration		24
36	5.1.2.1 [SDC-AUM-FH] Default configuration of authentication for functions whose use can cause harm ...		24
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.....		25
39	5.1.2.4 [SDC-FRM] Factory reset to restore the default state		25
40	5.1.2.5 [SDC-LOG-LOW] Default creation of events to log for low risk SHGPVA		25
41	5.1.3 Authentication and access control mechanisms		25
42	5.1.3.1 [ACM-FH] Access control for functions whose use can cause harm		25
43	5.1.3.2 [AUM-FH] Authentication for functions whose use can cause harm.....		26
44	5.1.3.3 [AUTHZ-LP] Least privilege in authorization policies.....		26
45	5.1.3.4 [AUTHZ-R] Revocability of granted permissions		26
46	5.1.4 Integrity protection.....		27
47	5.1.4.1 [INT-SWPCK] Software package verification		27
48	5.1.4.2 [INT-COM] Communication of integrity relevant data.....		27
49	5.1.5 Confidentiality protection		27
50	5.1.5.1 [CONF-SSM] Confidentiality protecting persistent storage for confidential data		27
51	5.1.5.2 [CONF-COM] Communication of confidential data.....		28
52	5.1.5.3 [CONF-MON-HW] Indication of active capture of audio or video data for hardware architectural		
53	component SHGPVA		28

54	5.1.5.4	[CONF-MON-UI] Indication of active capture of audio or video data for software architectural component SHGPVA with human interfaces.....	28
55			
56	5.1.5.5	[CONF-MON-API] Indication of active capture of audio or video data for software architectural component SHGPVA without a human interface.....	28
57			
58	5.1.5.6	[CONF-CAPT-MUTE] Mechanism to disable capture.....	28
59	5.1.5.7	[CONF-CAPT-MUTE-DISABLE] Allowing capturing after disabling.....	28
60	5.1.6	Data minimization.....	29
61	5.1.6.1	[DMIN-DJST] Documented justification of processed data.....	29
62	5.1.6.2	[DMIN-USERINFO] User Information about processing of audio- and video data.....	29
63	5.1.6.3	[DMIN-LOCAL] Local event detection.....	29
64	5.1.7	Availability protection.....	29
65	5.1.7.1	[AVAI-TIME-RECO-POW] Restoration after loss of power.....	29
66	5.1.7.2	[AVAI-TIME-NETW] Local operation.....	29
67	5.1.7.3	[AVAI-TIME-RECO-NETW] Restoration after loss of network connection.....	29
68	5.1.7.4	[AVAI-TIME-OUTA-NOT] Notify non-availability.....	30
69	5.1.7.5	[AVAI-TIME-PREV-NOT] Notify upcoming limitation.....	30
70	5.1.7.6	[AVAI-TIME-NET-PRIO] Network prioritization.....	30
71	5.1.7.7	[AVAI-TIME-RES-PRIO] Power resource prioritization.....	30
72	5.1.7.8	[AVAI-TIME-IMP-AMP] Amplification control.....	30
73	5.1.7.9	[AVAI-TIME-DOS-RATE] Incoming rate limiting.....	30
74	5.1.7.10	[AVAI-SUM-SCHEDULE] Scheduling of updates.....	31
75	5.1.8	Impact minimization.....	31
76	5.1.9	Limit attack surface.....	31
77	5.1.9.1	[LAS-INVAL] Validation of external data input.....	31
78	5.1.9.2	[LAS-INSAN] Sanitization of external data input.....	31
79	5.1.9.3	[LAS-PHY-INF] Only necessary physical interfaces.....	31
80	5.1.9.4	[LAS-LOGIC-INF] Only necessary logical interfaces active by default.....	31
81	5.1.9.5	[LAS-APP] Only necessary apps by default.....	31
82	5.1.9.6	[LAS-SBOOT] Secure boot.....	32
83	5.1.10	Logging and monitoring mechanisms.....	32
84	5.1.10.1	[LOG-LOW] Events to log for low risk SHGPVA.....	32
85	5.1.10.2	[LOG-MEDIUM] Events to log for medium risk SHGPVA.....	32
86	5.1.10.3	[LOG-HIGH] Events to log for high risk SHGPVA.....	32
87	5.1.10.4	[LOG-TIME] Timestamps for logs.....	33
88	5.1.10.5	[LOG-TIME-HIGH] Real-Timestamps for logs.....	33
89	5.1.10.6	[LOG-STORAGE] Persistently store logfiles.....	33
90	5.1.10.7	[LOG-BACKUP] Backup of logfiles.....	33
91	5.1.10.8	[LOG-USER-ACC] User access to logs concerning their privacy.....	33
92	5.1.11	Deletion mechanisms.....	33
93	5.1.11.1	[DLM-PERM] Permanent removal of user-related data.....	33
94	5.1.12	Other product's technical requirements specifications.....	34
95	5.1.12.1	[USERNOT-NOSECFUC] User notifications on not available security functions.....	34
96	5.1.12.2	[USERNOT-SECREL] Language and representation for security-related user notifications.....	34
97	5.1.12.3	[GUI-SECCONF] Visual representation of security-related configuration via GUIs.....	34
98	5.1.12.4	[CRY-SOTA] State-of-the-art cryptography.....	34
99	5.1.12.5	[CRY-CCK-PRE-LEN] Key size of preinstalled confidential cryptographic keys.....	34
100	5.1.12.6	[CRY-CCK-GEN] Default key size of generated confidential cryptographic keys.....	34
101	5.1.12.7	[CRY-PW-PRE-COM] Complexity of preinstalled passwords.....	35
102	5.1.12.8	[CRY-PW-GEN-COM] Default complexity of generated passwords.....	35
103	5.1.12.9	[CRY-PW-USR-COM] Recommended complexity of user chosen passwords.....	35
104	5.2	Requirements specifications for vulnerability handling activities related to the product.....	35
105	6	Assessing for compliance with requirements.....	35
106	6.1	Assessing for compliance with product's technical requirements specifications.....	35
107	6.1.1	General.....	35
108	6.1.2	Known exploitable vulnerabilities.....	35
109	6.1.2.1	Assessment criteria for [NKEV-SUM-SUPPORT].....	35
110	6.1.2.2	Assessment criteria for [NKEV-SUM-PROVIDE].....	37
111	6.1.2.3	Assessment criteria for [NKEV-SUM-AUTO].....	38
112	6.1.2.4	Assessment criteria for [NKEV-SUM-NOTIF].....	39
113	6.1.3	Default configuration.....	40

114	6.1.3.1	Assessment criteria for [SDC-AUM-FH]	40
115	6.1.3.2	Assessment criteria for [SDC-FRM]	41
116	6.1.4	Authentication and access control mechanisms	42
117	6.1.4.1	Assessment criteria for [ACM-FH]	42
118	6.1.4.2	Assessment criteria for [AUM-FH]	43
119	6.1.4.3	Assessment criteria for [AUTHZ-LP]	44
120	6.1.4.4	Assessment criteria for [AUTHZ-R]	45
121	6.1.5	Integrity protection	45
122	6.1.6	Confidentiality protection	45
123	6.1.7	Data minimization	45
124	6.1.7.1	Assessment criteria for [DMIN-DJST]	45
125	6.1.8	Availability protection	46
126	6.1.8.1	Assessment criteria for [AVAI-TIME-RECO-POW]	46
127	6.1.8.2	Assessment criteria for [AVAI-TIME-NETW]	48
128	6.1.8.3	Assessment criteria for [AVAI-TIME-RECO-NETW]	49
129	6.1.8.4	Assessment criteria for [AVAI-TIME-OUTA-NOT]	51
130	6.1.8.5	Assessment criteria for [AVAI-TIME-PREV-NOT]	52
131	6.1.8.6	Assessment criteria for [AVAI-TIME-NET-PRIO]	53
132	6.1.8.7	Assessment criteria for [AVAI-TIME-RES-PRIO]	54
133	6.1.8.8	Assessment criteria for [AVAI-TIME-IMP-AMP]	55
134	6.1.8.9	Assessment criteria for [AVAI-TIME-DOS-RATE]	56
135	6.1.8.10	Assessment criteria for [AVAI-SUM-SCHEDULE]	57
136	6.1.9	Impact minimization	59
137	6.1.10	Limit attack surface	59
138	6.1.10.1	Assessment criteria for [LAS-SBOOT]	59
139	6.1.11	Logging and monitoring mechanisms	60
140	6.1.11.1	Assessment criteria for [LOG-LOW]	60
141	6.1.11.2	Assessment criteria for [LOG-MEDIUM]	61
142	6.1.11.3	Assessment criteria for [LOG-HIGH]	62
143	6.1.11.4	Assessment criteria for [LOG-TIME]	63
144	6.1.11.5	Assessment criteria for [LOG-TIME-HIGH]	64
145	6.1.11.6	Assessment criteria for [LOG-STORAGE]	65
146	6.1.11.7	Assessment criteria for [LOG-BACKUP]	66
147	6.1.12	Deletion mechanisms	67
148	6.1.12.1	Assessment criteria for [DLM-PERM]	67
149	6.1.13	Other product's technical requirements specifications	68
150	6.1.13.1	Assessment criteria for [USERNOT-SECREL]	68
151	6.1.13.2	Assessment criteria for [GUI-SECCONF]	69
152	6.2	Assessment criteria for vulnerability handling activities related to the product	70
153	Annex A (informative):	Relationship between the present document and the requirements of	
154		EU Regulation 2024/2847	71
155	Annex B (informative):	Guidance for the application of the present document	77
156	Annex C (informative):	Information on the methodology for the assessment of cybersecurity	
157		risks used to develop the present document	81
158	C.1	Guidance for determining impact classes	81
159	C.1.1	General	81
160	C.1.2	confidential data	81
161	C.1.3	loss sensitive data	81
162	C.1.4	time sensitive data and time sensitive function	82
163	C.1.5	integrity relevant data and integrity relevant function	82
164	Annex D (normative):	Relationship between specific data and functions assets covered by	
165		the present document to impact classes for generic asset categories	84
166	D.1	Data assets	84
167	D.2	Function assets	85
168	Annex E (normative):	Protection measures	87
169	E.1	authentication mechanism strength	87

170	E.1.1	[AUM-FH] Authentication for functions whose use can cause harm	87
171	E.1.1.1	General	87
172	E.1.1.2	authentication - strength level basic	87
173	E.1.1.3	authentication - strength level normal	87
174	E.1.1.4	authentication - strength level enhanced.....	88
175	E.1.1.5	authentication - strength level strong.....	88
176	E.1.2	Assessment for authentication mechanism strength.....	89
177	E.1.2.1	Assessment criteria regarding the protection against limited presentation attacks.....	89
178	E.1.2.2	Assessment criteria regarding the protection against targeted presentation attacks	89
179	E.1.2.3	Assessment criteria regarding the protection against elaborate presentation attacks.....	90
180	E.1.2.4	Assessment criteria regarding the protection against limited brute force attacks.....	90
181	E.1.2.5	Assessment criteria regarding the protection against targeted brute force attacks.....	91
182	E.1.2.6	Assessment criteria regarding the protection against automated brute force attacks.....	92
183	E.1.2.7	Assessment criteria regarding the protection against presentation attacks	92
184	E.1.2.8	Assessment criteria regarding the protection against elaborate brute force attacks.....	93
185	E.1.2.9	Assessment criteria regarding the protection against automated security token spoofing attacks.....	94
186	E.1.2.10	Assessment criteria regarding the protection against targeted security token spoofing attacks.....	94
187	E.1.2.11	Assessment criteria regarding the protection against elaborate security token spoofing attacks.....	95
188	E.1.2.12	Assessment criteria regarding the protection against replay attacks.....	95
189	E.1.2.13	Assessment criteria regarding the protection against PitM attacks.....	96
190	E.2	integrity protection strength.....	97
191	E.2.1	[INT-SWPCK] Software package verification.....	97
192	E.2.1.1	General	97
193	E.2.1.2	software package integrity verification - strength level basic.....	97
194	E.2.1.3	software package integrity verification - strength level normal.....	97
195	E.2.1.4	software package integrity verification - strength level enhanced.....	97
196	E.2.2	[INT-COM] Communication of integrity relevant data	97
197	E.2.2.1	General	97
198	E.2.2.2	communication of integrity relevant data - protection strength level basic	97
199	E.2.2.3	communication of integrity relevant data - protection strength level normal	97
200	E.2.2.4	communication of integrity relevant data - protection strength level enhanced	98
201	E.2.2.5	communication of integrity relevant data - protection strength level strong	98
202	E.3	confidentiality protection strength	98
203	E.3.1	[CONF-SSM] Confidentiality protecting persistent storage for confidential data	98
204	E.3.1.1	General	98
205	E.3.1.2	confidential persistent storage - strength level basic	98
206	E.3.1.3	confidential persistent storage - strength level normal	98
207	E.3.1.4	confidential persistent storage - strength level enhanced.....	99
208	E.3.1.5	confidential persistent storage - strength level strong.....	99
209	E.3.2	[CONF-COM] Communication of confidential data.....	99
210	E.3.2.1	General	99
211	E.3.2.2	authentication - strength level strong.....	99
212	E.3.2.3	communication of confidential data - protection strength level normal	99
213	E.3.2.4	communication of confidential data - protection strength level enhanced.....	99
214	E.3.2.5	communication of confidential data - protection strength level strong.....	100
215	Annex F (informative):	Relationship between the present document and the covered/not	
216		covered cybersecurity risks.....	100
217	Annex G (informative):	Relationship between the present document and ETSI EN 303 645/	
218		ETSI TS 103 701	104
219			
220			

221 Intellectual Property Rights

222 Essential patents

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

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

232 Trademarks

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

237 **DECT™, PLUGTESTS™, UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its
 238 Members. **3GPP™, LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the
 239 3GPP Organisational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of
 240 the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

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

242 Foreword

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

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

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

252 Once the present document is cited in the Official Journal of the European Union under that Regulation, compliance
 253 with the normative clauses of the present document given in table A.1 confers, within the limits of the scope of the
 254 present document, a presumption of conformity with the corresponding requirements of that Regulation and associated
 255 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

256 Modal verbs terminology

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

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

261

262 1 Scope

263 The present document specifies vulnerability handling activities, technical requirements and corresponding assessment
 264 criteria for smart home general purpose virtual assistants related to cybersecurity. The products with digital elements in
 265 scope, thereafter "smart home general purpose virtual assistants":

- 266 • are specified within the "technical description" of the "category of product" number "16." by the Commission
 267 Implementing Regulation (EU) 2025/2392 [i.2] as:
 268 "Products with digital elements that communicate on the public Internet, whether directly or via other
 269 equipment, that process demands, tasks or questions based on natural language prompts, such as through audio
 270 or written input, and that, based on those demands, tasks or questions, provide access to other services or
 271 control the functions of connected devices in residential settings.
 272 This category includes but is not limited to smart speakers with an integrated virtual assistant, and standalone
 273 virtual assistants that meet this description." and
- 274 • are only covered within the product context described in clause 4.

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

277 2 References

278 2.1 Normative references

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

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

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

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

- 287 [1] CEN/CLC JT013090:2026 (CEN/CLC prEN 40000-1-3): "Cybersecurity requirements for
 288 products with digital elements - Vulnerability Handling".
- 289 [2] [Agreed Cryptographic Mechanisms](#): "European Union Agency for Cybersecurity, European
 290 Cybersecurity Certification Group - Sub-group on Cryptography - Agreed Cryptographic
 291 Mechanisms".

292 2.2 Informative references

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

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

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

- 300 [i.1] [Regulation \(EU\) 2024/2847](#): "Regulation (EU) 2024/2847 of the European Parliament and of the
 301 Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital
 302 elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU)
 303 2020/1828 (Cyber Resilience Act)".

- 304 [i.2] [Regulation \(EU\) 2025/2392](#): "Commission Implementing Regulation (EU) 2025/2392 of 28
305 November 2025 on the technical description of the categories of important and critical products
306 with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of
307 the Council".
- 308 [i.3] [Standardisation request M/606 - C\(2025\)618](#): "Commission Implementing decision of 3.2.2025 on
309 a standardisation request to the European Committee for Standardisation (CEN), the European
310 Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications
311 Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU)
312 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal
313 cybersecurity requirements for products with digital elements and amending Regulations (EU) No
314 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)".
- 315 [i.4] CEN/CLC JT013095:2026 (CEN/CLC prEN 40000-1-1): "Cybersecurity requirements for
316 products with digital elements – Vocabulary".
- 317 [i.5] ETSI EN 304 623 vx.x.x: "Cyber Security (CYBER); CRA; Cybersecurity requirements for boot
318 managers".
- 319 [i.6] [ISO/IEC 24760-1:2025](#): "Information security, cybersecurity and privacy protection — A
320 framework for identity management - Part 1: Core concepts and terminology".

321 3 Definition of terms, symbols and abbreviations

322 3.1 Terms

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

325 ARCHITECTURE RELATED TERMS

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

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

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

332 **architectural component**: self-contained hardware architectural component or software architectural component that is
333 part of the SHGPVA

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

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

338 **hardware architectural component**: self-contained hardware part of the SHGPVA including its associated software
339 architectural component

340 EXAMPLE: virtual assistant hardware device

341 **software architectural component**: self-contained software part of the SHGPVA

342 EXAMPLE 1: Companion-App, RDPS-Cloud-Application

343 EXAMPLE 2: virtual assistant software

344 ASSET CATEGORIES

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

346 **data asset**: asset, that is data processed by the SHGPVA

347 **function asset**: asset, that is a function of the SHGPVA

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

- 349 • a function, whose use can impact the availability of other devices, services or networks,
- 350 • a function, whose use can impact the safety or privacy of human entities,
- 351 • a function, which can communicate confidential data,
- 352 • a function, which can communicate integrity relevant data,
- 353 • a function, which can modify integrity relevant data, or
- 354 • a function, which can modify integrity relevant functions

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

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

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

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

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

360 COMMUNICATION TYPES

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

363 EXAMPLE: communication through a virtual-private-network tunnel with a communication partner in a private
364 network

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

367 EXAMPLE: point to point communication via short-range wireless technologies between two communication
368 partners.

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

371 EXAMPLE: direct communication with a chip after modification on a SHGPVA's hardware architectural
372 component

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

374 EXAMPLE: communication via internet

375 **strict local communication:** ingoing/outgoing communication which requires physical presence at the communication
376 partner

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

378 DATA ASSETS

379 **SHGPVA state data:** data asset that contains SHGPVA state information

380 **activity data:** data asset that describes physical movements, behaviors or activity patterns to monitor the personal
381 fitness level of humans

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

383 **audio input data:** data asset that represents audio information captured by the SHGPVA

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

385 EXAMPLE: assignment of privileges to users

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

387 EXAMPLE: passwords, data hashes, message authentication codes, keys used for symmetric or asymmetric
388 cryptography, (pseudo-)random numbers
389 **device location data:** data asset containing information on the geographical information of devices

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

391 **health data:** data asset that indicates information about physiological functions, health condition or physical fitness of
392 humans

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

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

395 **personal calendar data:** data asset that represents information on a personal calendar

396 **personal contact data:** data asset that represents personal contact information of entities

397 **personal notes data:** data asset that represents personal information where the content is not specified by the
398 manufacturer but can be freely filled by the user

399 NOTE: personal notes data is typically obtained via note keeping applications e.g. for shopping lists or personal
400 memoranda.

401 **public data asset:** data asset derived from public data

402 **software package:** data asset that contains software intended to be installed on the SHGPVA

403 **video input data:** data asset that represents video information captured by the SHGPVA

404 EXAMPLE: video or picture recordings processed (including storage) on the SHGPVA

405 **DATA RELATED TERMS**

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

408 EXAMPLE: symmetric keys, private keys
409 NOTE: A confidential cryptographic key is a cryptographic security parameter

410 **data:** information in digital form

411 **location data:** data containing geographical information

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

414 EXAMPLE: symmetric keys, private keys
415 NOTE 1: "A password is a cryptographic security parameter"

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

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

419 **processed data:** data processed by the SHGPVA, including but not limited to capturing, storing, transmitting,
420 modifying, deleting and presenting data

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

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

423 **FUNCTION ASSETS**

424 **access control mechanism:** SHGPVA function that enforces an authorization policy

425 EXAMPLE: the function to ensure, that no unauthorized entity gains access to the identification management
426 function in an alarm system.

- 427 **actuator control function:** function asset intended to control an actuator function
- 428 **audio input function:** SHGPVA function that converts audio signals into data
- 429 **audio output function:** SHGPVA function that converts data into audio signals
- 430 **authentication mechanism:** SHGPVA function that verifies an entity's claimed identity
- 431 EXAMPLE: the authentication function of an alarm system for credential verification
- 432 **bootloader function:** SHGPVA function that initiates the execution of other core software at start up.
- 433 **configuration function:** SHGPVA function that allows to change the configuration of SHGPVA's functions
- 434 EXAMPLE: user identification management function in an alarm system
- 435 **connection function:** SHGPVA function that is used for testing or establishing communication capability via machine
- 436 interface
- 437 EXAMPLE: ICMP, DHCP Discovery
- 438 NOTE: In this context, establishing communication means communication without user-related data and without
- 439 authentication of the communication partner for the purpose of establishment of a connection.
- 440 **cryptographic function:** SHGPVA function that performs cryptographic algorithm
- 441 **data backup mechanism:** SHGPVA function that copies data assets to persistent storage of another architectural
- 442 component or target outside the SHGPVA.
- 443 **data presenting function:** SHGPVA function that grants an entity read access to data or presents data to a user via
- 444 physical human interface
- 445 EXAMPLE 1: Presenting data to a user on a website associated with a RDPS
- 446 EXAMPLE 2: Presenting data on a display, controlling indicator lights
- 447 **factory reset function:** SHGPVA function that removes all user-related data and sets the architectural components in a
- 448 factory default state, potentially keeping software updates
- 449 **input sanitization mechanism:** SHGPVA function that scans function input data based on a function specific pattern
- 450 and removes or alters parts, that can lead to incidents
- 451 EXAMPLE: If external data input is amongst others intended to be stored via a database service, escape
- 452 characters and other database service specific commands (defined by a corresponding function
- 453 specific pattern) are removed from the external data input, before it is processed by the database
- 454 service.
- 455 **input validation mechanism:** SHGPVA function that rejects input data if it does not meet an accepted pattern
- 456 EXAMPLE: The input is expected to be the users' year of birth. Data type validation is used to ensure the input
- 457 to be an integer followed by a range validation checking that the input is between 1900 and the
- 458 current year.
- 459 **logging mechanism:** SHGPVA function that logs events
- 460 **monitoring mechanism:** SHGPVA function that frequently measures functional metrics of the SHGPVA
- 461 **notification mechanism:** SHGPVA function that notifies entities on certain events
- 462 **real-time service or clock:** service or function that provides real time information
- 463 **sensing function:** SHGPVA function to measure characteristics of its physical operational environment
- 464 **software package verification mechanism:** SHGPVA function that verifies the integrity and authenticity of software
- 465 packages
- 466 **software update mechanism:** SHGPVA function that receives and installs software updates
- 467 **time service or function:** service or function that provides time information
- 468 **video input function:** SHGPVA function that converts video signals into data

469 **video output function:** SHGPVA function that converts data into video signals

470 FUNCTION RELATED TERMS

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

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

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

475 EXAMPLE 2: A hardware architectural component with only local communication capabilities receives the
476 update from another architectural component in its proximity. The other architectural component
477 has a connection to the internet and downloads the software for the hardware architectural
478 component without user interaction. The hardware architectural component can only be
479 automatically updated when the other architectural component is in its proximity.

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

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

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

- 485 • a modification or creation of SHGPVAs' data or functions
- 486 • information intended to inform human users
- 487 • information intended to inform or control devices or services, or
- 488 • an action on the physical operational environment

489 NOTE: function output that is an action on the physical operational environment can be performed by a
490 SHGPVA's actuator function.

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

- 492 • human users,
- 493 • devices or services, or
- 494 • the physical operational environment

495 NOTE: function trigger input provided by the physical operational environment can be received by a SHGPVA's
496 sensing function.

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

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

499 **virtual assistant function:** SHGPVA function which provides function output as reaction to function trigger input
500 related to assistance of a user and can process natural language prompts

501 INTERFACES

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

503 EXAMPLE: PIN pad, touch screen, web interface for user login and user product management

504 **interface:** shared boundary across which the SHGPVA exchanges information

505 **logical human interface:** interface that is a human interface and a logical interface

506 EXAMPLE: web page for remote access

507 NOTE: An external client used for remote access providing a logical human interface typically uses a machine
508 interface to communicate with the SHGPVA

509 **logical interface:** interface that does not exist in hardware and can only be used by using another device or a physical
510 interface of a SHGPVA

511 **machine interface:** interface that is intended to be used for machine-to-machine communication

512 EXAMPLE 1: Interfaces for USB/Bluetooth®/Ethernet/Wi-Fi®/DECT/DECT-2020 NR or debug ports
513 accessible from outside the SHGPVA

514 EXAMPLE 2: tag reader, keyfob radio interface, wired or radio interface (for installation or maintenance),
515 transmitter interface to the network, endpoint interface, digital interface to components of an alarm
516 system

517 **physical human interface:** interface that is a human interface and a physical interface

518 EXAMPLE: keypad, display, biometric reader, microphone, loudspeaker, (video) camera, touchscreen

519 **physical interface:** interface that is part of the hardware of a SHGPVA

520 EXAMPLE: USB/RJ45/JTAG ports, microSD/SIM card slot

521 OPERATIONAL ENVIRONMENTS

522 **confined operational environment:** physical operational environment, where the geographical location is confined to a
523 specific area

524 **fully controlled physical operational environment:** physical operational environment, where physical access is fully
525 controlled by the user or trusted persons

526 EXAMPLE: private house or apartment

527 **logical operational environment:** operational environment describing the accessibility via logical interfaces

528 **mobile operational environment:** physical operational environment, where the geographical location is changing
529 during operation and not confined to a specific area

530 NOTE: Physical operational environment of smartphones and wearables

531 **operational environment:** System used to model to likelihood of incidents depending on the physical operational
532 environment of the SHGPVA, or parts of it, and the logical operational environment of the relevant logical interfaces.

533 **partially controlled physical operational environment:** physical operational environment, that is not a fully
534 controlled physical operational environment and either under the control of a limited set of persons or located in an area
535 where untrusted physical access is suspicious

536 EXAMPLE: Shared area in a house with different apartments or private property where public access is not
537 intended.

538 **physical operational environment:** operational environment determining the physical accessibility of an architectural
539 component

540 **stationary operational environment:** physical operational environment, where the geographical location is fixed

541 **uncontrolled physical operational environment:** physical operational environment, where physical access control on
542 arbitrary untrusted entities cannot be ensured for prolonged time periods and where untrusted physical access is not
543 necessarily suspicious

544 EXAMPLE: Areas intended for public access

545 USERS

546 **user:** natural entity that directly interacts with the SHGPVA

547 NOTE: This includes all natural entities that interact directly with the SHGPVA as the final product, but not
548 manufactures for integration in other products.

549 3.2 Abbreviations

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

551 GENERAL

552	DHCP	Dynamic Host Configuration Protocol
553	GPS	Global Positioning System
554	GUI	Graphical User Interface
555	ICMP	Internet Control Message Protocol
556	RDPS	Remote Data Processing Solution
557	USB	Universal Serial Bus
558	VAF	Virtual Assistant Function
559	SHGPVA	Smart Home General Purpose Virtual Assistant

560 COMMUNICATION TYPES

561	COM	communication type
562	COM.Adjacent	adjacent communication
563	COM.Any	unspecified communication type
564	COM.Local	local communication
565	COM.Physical	physical communication
566	COM.Public	public communication
567	COM.StrictLocal	strict local communication

568 IMPACT CLASSES

569	IMP	impact class
570	IMP.AVAI.LOSS	loss sensitive availability impact class
571	IMP.AVAI.LOSS.High	loss sensitive availability impact class high
572	IMP.AVAI.LOSS.Low	loss sensitive availability impact class low
573	IMP.AVAI.LOSS.Medium	loss sensitive availability impact class medium
574	IMP.AVAI.TIME	time sensitive availability impact class
575	IMP.AVAI.TIME.High	time sensitive availability impact class high
576	IMP.AVAI.TIME.Low	time sensitive availability impact class low
577	IMP.AVAI.TIME.Medium	time sensitive availability impact class medium
578	IMP.CONF	confidentiality impact class
579	IMP.CONF.High	confidentiality impact class high
580	IMP.CONF.Low	confidentiality impact class low
581	IMP.CONF.Medium	confidentiality impact class medium
582	IMP.FH	impact class for function, whose use can cause harm
583	IMP.FH.CCON	function, which can communicate confidential data impact class
584	IMP.FH.CCON.High	function, which can communicate confidential data impact class high
585	IMP.FH.CCON.Low	function, which can communicate confidential data impact class low
586	IMP.FH.CCON.Medium	function, which can communicate confidential data impact class medium
587	IMP.FH.DSN	function, whose use can impact the availability of other devices, services or networks impact class
588	IMP.FH.DSN.High	function, whose use can impact the availability of other devices, services or networks impact class high
589	IMP.FH.DSN.Low	function, whose use can impact the availability of other devices, services or networks impact class low
590	IMP.FH.DSN.Medium	function, whose use can impact the availability of other devices, services or networks impact class medium
591	IMP.FH.High	function, whose use can cause harm impact class high
592	IMP.FH.Low	function, whose use can cause harm impact class low
593	IMP.FH.MINT	function, which can modify integrity relevant data impact class
594	IMP.FH.MINT.High	function, which can modify integrity relevant data impact class high
595	IMP.FH.MINT.Low	function, which can modify integrity relevant data impact class low
596	IMP.FH.MINT.Medium	function, which can modify integrity relevant data impact class medium
597	IMP.FH.Medium	function, whose use can cause harm impact class medium
598	IMP.FH.SP	function, whose use can impact the safety or privacy of human entities impact class
599	IMP.FH.SP.High	function, whose use can impact the safety or privacy of human entities impact class high
600	IMP.FH.SP.Low	function, whose use can impact the safety or privacy of human entities impact class low
601	IMP.FH.SP.Medium	function, whose use can impact the safety or privacy of human entities impact class medium
602	IMP.High	impact class high
603	IMP.INT	integrity impact class
604	IMP.INT.High	integrity impact class high
605	IMP.INT.Low	integrity impact class low
606	IMP.INT.Medium	integrity impact class medium
607	IMP.Low	impact class low

611 IMP.Medium impact class medium

612 **INTERFACES**

613 IF interface

614 IF.Any unspecified interface

615 IF.Human human interface

616 IF.HumanLogical logical human interface

617 IF.HumanPhysical physical human interface

618 IF.Logical logical interface

619 IF.Machine machine interface

620 IF.Physical physical interface

621 **OPERATIONAL ENVIRONMENTS**

622 POE physical operational environment

623 POE.Any unspecified physical operational environment

624 POE.Confined confined operational environment

625 POE.FullyControlled fully controlled physical operational environment

626 POE.Mobile mobile operational environment

627 POE.PartiallyControlled partially controlled physical operational environment

628 POE.Stationary stationary operational environment

629 POE.Uncontrolled uncontrolled physical operational environment

630 **PROTECTION MEASURE STRENGTH LEVEL**

631 AUTH.Basic authentication - strength level basic

632 AUTH.Enhanced authentication - strength level enhanced

633 AUTH.Normal authentication - strength level normal

634 AUTH.Strong authentication - strength level strong

635 CONF.COM.Basic authentication - strength level strong

636 CONF.COM.Enhanced communication of confidential data - protection strength level enhanced

637 CONF.COM.Normal communication of confidential data - protection strength level normal

638 CONF.COM.Strong communication of confidential data - protection strength level strong

639 CONF.SSM.Basic confidential persistent storage - strength level basic

640 CONF.SSM.Enhanced confidential persistent storage - strength level enhanced

641 CONF.SSM.Normal confidential persistent storage - strength level normal

642 CONF.SSM.Strong confidential persistent storage - strength level strong

643 INT.COM.Basic communication of integrity relevant data - protection strength level basic

644 INT.COM.Enhanced communication of integrity relevant data - protection strength level enhanced

645 INT.COM.Normal communication of integrity relevant data - protection strength level normal

646 INT.COM.Strong communication of integrity relevant data - protection strength level strong

647 INT.SW.VER.Basic software package integrity verification - strength level basic

648 INT.SW.VER.Enhanced software package integrity verification - strength level enhanced

649 INT.SW.VER.Normal software package integrity verification - strength level normal

650 INT.SW.VER.Strong software package integrity verification - strength level strong

651 N/A not applicable

652 **4 Product context**

653 **4.1 Product functions**

654 **4.1.1 Virtual assistant functions**

655 The present document addresses the following essential functionalities of SHGPVA:

- 656 • **VAFs** that might make use of the following functions:

657 - audio input function

658 - video input function

659 - audio output function

- 660 - video output function
- 661 - SHGPVA function which can communicate SHGPVA data
- 662 - SHGPVA function which can modify SHGPVA data

663 4.1.2 Supporting functions

664 The present document addresses the following supporting functionalities of SHGPVA:

- 665 • configuration function
- 666 • software update mechanism
- 667 • monitoring mechanism
- 668 • notification mechanism
- 669 • logging mechanism
- 670 • access control mechanism
- 671 • authentication mechanism
- 672 • factory reset function
- 673 • integrity protecting communication mechanism
- 674 • confidentiality protecting communication mechanism
- 675 • integrity protecting secure storage mechanism
- 676 • confidentiality protecting secure storage mechanism
- 677 • deletion mechanism
- 678 • onboarding mechanism
- 679 • input sanitization mechanism
- 680 • input validation mechanism
- 681 • software package verification mechanism
- 682 • bootloader function
- 683 • time service or function
- 684 • real-time service or clock
- 685 • cryptographic function
- 686 • data backup mechanism

687 4.1.3 Data assets

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

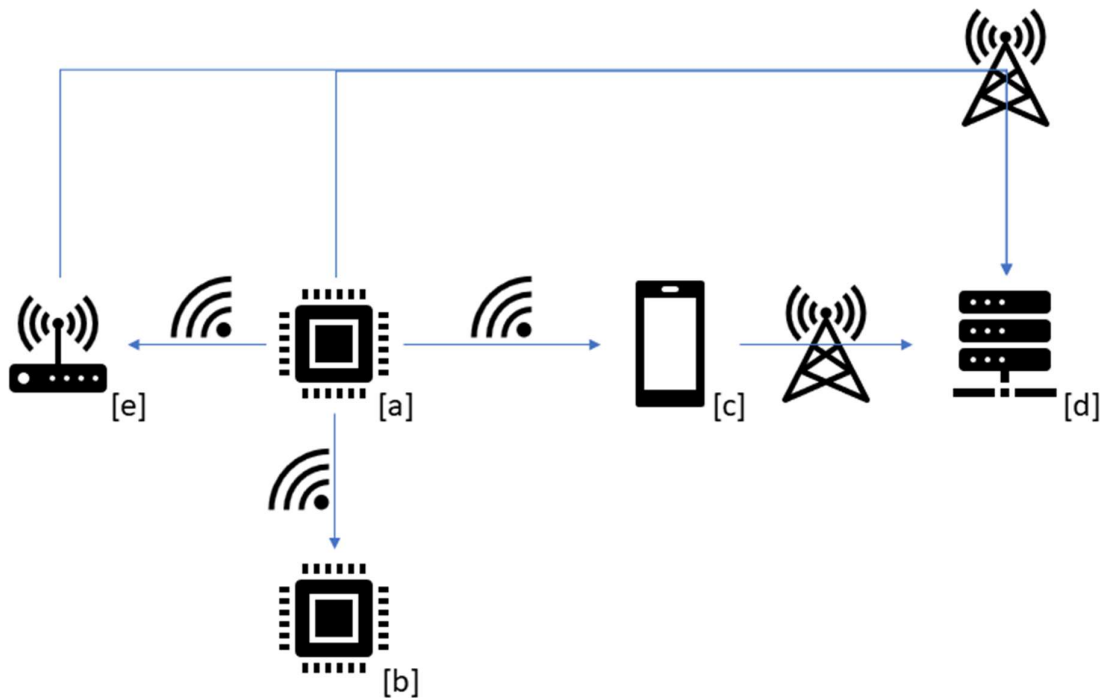
- 689 • SHGPVA state data
- 690 • activity data
- 691 • actuator control data
- 692 • audio input data

- 693 • authorization policy data
- 694 • cryptographic security parameter
- 695 • device location data
- 696 • function configuration data
- 697 • health data
- 698 • logging data
- 699 • network status data
- 700 • personal calendar data
- 701 • personal contact data
- 702 • personal notes data
- 703 • public data asset
- 704 • software package
- 705 • video input data

706 4.2 Product Architecture

707 The architecture of a SHGPVA consists of hardware architectural components and/or software architectural
708 components.

709 NOTE: It is possible that a SHGPVA consists of only one hardware architectural component.



710

711

Figure 1: Architectural Components and possible connections between them

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

- 714 (a) SHGPVA's hardware architectural component
- 715 (b) Another product's hardware architectural component
- 716 (c) SHGPVA's mobile application (software architectural component) installed on a smartphone
- 717 (d) SHGPVA's cloud RDPS (software architectural component) installed on a server
- 718 (e) SHGPVA's gateway (hardware architectural component)

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

721 4.3 Operational Environment

722 The present document addresses the following operational environments of SHGPVA.

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

- 725 • **public communication** - COM.Public,
- 726 • **adjacent communication** - COM.Adjacent,
- 727 • **local communication** - COM.Local,
- 728 • **strict local communication** - COM.StrictLocal.

729 The following physical operational environments are addressed for any hardware architectural component of the
730 SHGPVA:

- 731 • **fully controlled physical operational environment** - POE.FullyControlled,
- 732 • **partially controlled physical operational environment** - POE.PartiallyControlled,
- 733 • **mobile operational environment** - POE.Mobile.

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

- 736 • **fully controlled physical operational environment** - POE.FullyControlled,
- 737 • **partially controlled physical operational environment** - POE.PartiallyControlled,
- 738 • **mobile operational environment** - POE.Mobile.

739 4.4 Interfaces

740 The present document addresses the following interfaces of the SHGPVA:

- 741 • **human interface** - IF.Human
- 742 • **machine interface** - IF.Machine
- 743 • **logical interface** - IF.Logical
- 744 • **physical interface** - IF.Physical

745 4.5 Distribution of security functions

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

749 "The SHGPVA shall [...] use [some expression related to security functions]" means:

- 750 • the SHGPVA itself provides those security functions which are always used, or
- 751 • other products with digital elements in the SHGPVA's context provide those security functions which are
752 always used by the SHGPVA.

753 "The SHGPVA shall [...] support [some expression related to security functions]" means:

- 754 • the SHGPVA itself provides those security functions, or
- 755 • other products with digital elements in the SHGPVA's context provide those security functions.

756 "The SHGPVA shall [...] provide [some expression related to security functions]" means that the SHGPVA itself
757 provides those security functions.

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

761 4.6 Users

762 The present document addresses the following using entities of SHGPVA:

- 763 • Consumers for private usage
- 764 • Manufactures for integration in other products with digital elements intended for consumers

765 4.7 Use cases

766 4.7.1 General

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

768 4.7.2 Use case profiles

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

772 Use case profile for low impact functions

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

775 Example use cases:

776 The usage of a SHGPVA to access information that is derived from public data.

777 Use case profile for medium impact functions

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

780 Example use cases:

781 The usage of a SHGPVA:

- 782 • to access information that is derived from general user-related data or
- 783 • to modify general user-related data.

784 Use case profile for high impact functions

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

787 Example use cases:

788 The usage of a SHGPVA to access information that is derived from a user's health data.

789 4.8 Security Profiles

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

- 792 • security profile for low impact functions
- 793 • security profile for medium impact functions
- 794 • security profile for high impact functions

795

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
[SDC-LOG-LOW]	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
[CONF-MON-HW]	X	X	X
[CONF-MON-UI]	X	X	X
[CONF-MON-API]	X	X	X
[CONF-CAPT-MUTE]	X	X	X
[CONF-CAPT-MUTE-DISABLE]	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
[DMIN-USERINFO]	X	X	X
[DMIN-LOCAL]	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
[LOG-USER-ACC]	X	X	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

796 5 Requirements specifications

797 5.1 Product's technical requirements specifications

798 5.1.1 Known exploitable vulnerabilities

799 5.1.1.1 [NKEV-MKAV] No known exploitable vulnerabilities

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

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

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

807 5.1.1.2 [NKEV-SUM-SUPPORT] Secure software update mechanism

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

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

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

814 5.1.1.3 [NKEV-SUM-PROVIDE] Secure software update mechanism for core 815 components

816 All architectural components of the SHGPVA that include core software shall provide software update mechanisms,
817 that allow to update every part of the architectural components software, except for parts of the architectural
818 components software, that are immutable due to security.

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

820 5.1.1.4 [NKEV-SUM-AUTO] Automated security updates

821 Where the SHGPVA has the capability to connect to a public network, the SHGPVA shall support the automated update
822 of its software.

823 5.1.1.5 [NKEV-SUM-NOTIF] Update notifications

824 Where the SHGPVA has the capability to connect to a public network, the SHGPVA shall support the automated
825 notification of its users, when updates of its software are available.

826 5.1.2 Default configuration

827 5.1.2.1 [SDC-AUM-FH] Default configuration of authentication for functions whose 828 use can cause harm

829 The SHGPVA shall by default be configured to use authentication mechanisms that meet

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

832 except for connection functions.

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

834 5.1.2.2 [SDC-SUM-AUTO] Default configuration of automated security updates

835 Where

- 836 • the SHGPVA has the capability to connect to a public network; and
- 837 • no time sensitive function with IMP.AVAL.TIME.High is provided by an architectural component,

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

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

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

843 5.1.2.3 [SDC-SUM-NOTIF] Default configuration of update notifications

844 The SHGPVA shall by default be configured to use automated notification of its users, when updates of the SHGPVA's
845 software are available.

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

847 5.1.2.4 [SDC-FRM] Factory reset to restore the default state

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

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

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

854 5.1.2.5 [SDC-LOG-LOW] Default creation of events to log for low risk SHGPVA

855 Where the SHGPVA has a function, whose use can cause harm of impact class low as its highest function impact class,
856 the SHGPVA shall by default be configured to use logging mechanisms to create audit events for every:

- 857 • errors of the core software;
- 858 • capturing of audio or video data by an architectural component;
- 859 • storage of captured audio or video data, or data derived thereof.

860 5.1.3 Authentication and access control mechanisms

861 5.1.3.1 [ACM-FH] Access control for functions whose use can cause harm

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

864

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	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

			Impact class for function, whose use can cause harm		
			IMP.FH.Low	IMP.FH.Medium	IMP.FH.High
	COM.Local via a non-IF.HumanPhysical	POE.PartiallyControlled	applicable	applicable	applicable
		POE.Mobile	applicable	applicable	applicable
		POE.Any	applicable	applicable	applicable
	COM.Adjacent via IF.Any	applicable	applicable	applicable	
	COM.Public via IF.Any	applicable	applicable	applicable	

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

- 867 • factory reset function

868 5.1.3.2 [AUM-FH] Authentication for functions whose use can cause harm

869 The SHGPVA shall support authentication mechanisms, to authenticate entities using functions whose use can cause
870 harm before generating function output, where

- 871 • the authentication mechanisms strengths' are specified in clause [E.1.1](#) and
- 872 • the minimal required authentication strength is determined by table [3](#),

873 except for connection functions.

874 **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	COM.Local via a non-IF.HumanPhysical	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

875 For protection measures that are labelled with [*] it is not required that the SHGPVA uses authentication mechanisms
876 for its following functions:

- 877 • factory reset function

878 5.1.3.3 [AUTHZ-LP] Least privilege in authorization policies

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

880 NOTE: A SHGPVA whose intended purpose justifies not to differentiate between different user roles, can grant
881 all necessary permissions to the user.

882 5.1.3.4 [AUTHZ-R] Revocability of granted permissions

883 The SHGPVA shall support the revocation of any permission granted by an authorized entity.

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

885 5.1.4 Integrity protection

886 5.1.4.1 [INT-SWPCK] Software package verification

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

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

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

		Highest IMP.INT of the SHGPVA'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

893 5.1.4.2 [INT-COM] Communication of integrity relevant data

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

897 **Table 5: Assignment of protection mechanisms strength level for the integrity protection of outgoing**
898 **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	
	COM.Adjacent via IF.Any	POE.Any	POE.Mobile	INT.COM.Basic	INT.COM.Normal	INT.COM.Enhanced
			INT.COM.Enhanced	INT.COM.Enhanced	INT.COM.Enhanced	
COM.Public via IF.Any		INT.COM.Enhanced	INT.COM.Enhanced	INT.COM.Enhanced		

899 5.1.5 Confidentiality protection

900 5.1.5.1 [CONF-SSM] Confidentiality protecting persistent storage for confidential 901 data

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

905 **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

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

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

909 5.1.5.2 [CONF-COM] Communication of confidential data

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

913 **Table 7: Assignment of protection mechanisms strength level for the confidentiality of**
 914 **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 confidential data	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
	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

915 5.1.5.3 [CONF-MON-HW] Indication of active capture of audio or video data for 916 hardware architectural component SHGPVA.

917 Where the SHGPVA performs event-detection based on continuously captured audio or video data on a hardware
 918 architectural component, the SHGPVA shall use a visual or auditory indicator, to indicate to the user, in real time, when
 919 captured data is processed beyond the event-detection loop, on this hardware architectural component.

920 5.1.5.4 [CONF-MON-UI] Indication of active capture of audio or video data for 921 software architectural component SHGPVA with human interfaces.

922 Where the SHGPVA performs event-detection based on continuously captured audio or video data on a software
 923 architectural component that has a human interface, the SHGPVA shall use a visual or auditory indicator, to indicate to
 924 the user, in real time, when captured data is processed beyond the event-detection loop, on this software architectural
 925 components human interface.

926 5.1.5.5 [CONF-MON-API] Indication of active capture of audio or video data for 927 software architectural component SHGPVA without a human interface.

928 Where the SHGPVA performs event-detection based on continuously captured audio or video data on a software
 929 architectural component that has no human interface, the SHGPVA shall provide an API method, to indicate to the user,
 930 in real time, when captured data is processed beyond the event-detection loop via a machine interface of this software
 931 architectural component.

932 5.1.5.6 [CONF-CAPT-MUTE] Mechanism to disable capture

933 Where the SHGPVA has a sensing function to capture audio data or video data, the SHGPVA shall provide a
 934 mechanism to inhibit the capture of audio or video data.

935 EXAMPLE: camera cover, switch that disconnects the microphone

936 5.1.5.7 [CONF-CAPT-MUTE-DISABLE] Allowing capturing after disabling

937 Where the SHGPVA has a sensing function on a hardware architectural component to capture audio data or video data,
 938 the SHGPVA shall provide a physical human interface of the corresponding hardware architectural component as to
 939 sole way to disable the capture inhibition mechanism.

940 EXAMPLE: The capturing of audio can be disabled via app. To allow the capture again, a button on the
 941 hardware architectural component needs to be pressed.

942 NOTE: Disable the mechanism means allowing capture.

943 5.1.6 Data minimization

944 5.1.6.1 [DMIN-DJST] Documented justification of processed data

945 The SHGPVA shall only process confidential data according to its intended purpose.

946 EXAMPLE: The SHGPVA provides documentation that specifies the conditions under which audio or video
947 data is captured, stored, or transmitted when connected to the intended purpose. The data is
948 processed only in the cases specified in the documentation.

949 5.1.6.2 [DMIN-USERINFO] User Information about processing of audio- and video 950 data.

951 Where the SHGPVA processes audio input data or video input data, the SHGPVA shall provide information for its
952 users, in a easily understandable language, about:

- 953 • under which conditions the SHGPVA captures data;
- 954 • under which conditions the SHGPVA transmits captured data;
- 955 • under which conditions the SHGPVA transmits data derived from captured data;
- 956 • under which conditions the SHGPVA stores captured data;
- 957 • under which conditions the SHGPVA stores data derived from captured data;
- 958 • for how long stored data will be stored.

959 5.1.6.3 [DMIN-LOCAL] Local event detection

960 Where the SHGPVA monitors captured audio or video data to detect events to trigger further processing of these data,
961 the SHGPVA shall not use interface of public communication to transfer these data, even between its architectural
962 components, before such an event has been detected.

963 EXAMPLE: A SHGPVA consist of several "microphone units" which transmit their captured audio data to a
964 central "processing unit" via (W)LAN, where event detection takes place. The SHGPVA makes
965 sure, that its "units" are in the same broadcast domain before allowing transfer.

966 NOTE: It is permitted that a multi-step event detection pipeline is used, where a coarse event detection is
967 performed locally and further detection and processing is performed on a cloud RDPS.

968 5.1.7 Availability protection

969 5.1.7.1 [AVAI-TIME-RECO-POW] Restoration after loss of power

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

972 5.1.7.2 [AVAI-TIME-NETW] Local operation

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

975 5.1.7.3 [AVAI-TIME-RECO-NETW] Restoration after loss of network connection

976 The SHGPVA shall use a mechanism to attempt to reconnect cleanly after a loss of network connection.

977 EXAMPLE: A SHGPVA loses connection to the local network as the network is temporarily unavailable. After
978 recognizing the restored network, the SHGPVA reconnects after a randomized delay to reconnect
979 cleanly.

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

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

984 5.1.7.4 [AVAI-TIME-OUTA-NOT] Notify non-availability

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

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

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

993 5.1.7.5 [AVAI-TIME-PREV-NOT] Notify upcoming limitation

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

997 EXAMPLE: A battery powered SHGPVA recognizes low battery and sends a notification to the user.

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

999 5.1.7.6 [AVAI-TIME-NET-PRIO] Network prioritization

1000 Where at least one time sensitive function with IMP.AVAI.TIME.Medium or higher with the need of network
 1001 connectivity for its operation is provided by the SHGPVA, the SHGPVA shall use a mechanism to prioritize its use of
 1002 network resources in case of a network resource conflict:

- 1003 • such that these functions are prioritized according to their IMP.AVAI.TIME.High; or
- 1004 • such that functions are prioritized according to user decisions or configuration.

1005 5.1.7.7 [AVAI-TIME-RES-PRIO] Power resource prioritization

1006 Where

- 1007 • at least one time sensitive function with IMP.AVAI.TIME.Medium or higher is provided by the SHGPVA;
 1008 and
- 1009 • the SHGPVA is intended to be powered by battery,

1010 the SHGPVA shall use a mechanism to prioritize use of power in the case of a low power condition:

- 1011 • such that these functions are prioritized according to their IMP.AVAI.TIME; or
- 1012 • such that functions are prioritized according to user decisions or configuration.

1013 5.1.7.8 [AVAI-TIME-IMP-AMP] Amplification control

1014 Where at least one function, whose use can impact the availability of other devices, services or networks with
 1015 IMP.FH.DSN.Medium or higher is provided by the SHGPVA, the SHGPVA shall use mechanisms to prevent effective
 1016 amplification of requests or network traffic of these functions.

1017 EXAMPLE: An ICMP request has an amplification factor of three. Then the response time is artificially
 1018 extended by a factor of tree per destination to have no effective gain in bandwidth.

1019 5.1.7.9 [AVAI-TIME-DOS-RATE] Incoming rate limiting

1020 Where at least one time sensitive function with IMP.AVAI.TIME.High AND at least one machine interface are
 1021 provided by the SHGPVA, the SHGPVA shall use mechanisms to discard packets from a source if it sends an unusually
 1022 high number of requests, whose execution could result in a resource conflict.

1023 **5.1.7.10 [AVAI-SUM-SCHEDULE] Scheduling of updates**

1024 Where

- 1025 • the SHGPVA has the capability to connect to a public network; and
- 1026 • at least one time sensitive function with IMP.AVAI.TIME.Medium or higher is provided by an architectural
1027 component,

1028 the SHGPVA shall support the scheduling of the application of updates of those architectural components.

1029 **5.1.8 Impact minimization**

1030 **5.1.9 Limit attack surface**

1031 **5.1.9.1 [LAS-INVAL] Validation of external data input**

1032 The SHGPVA shall use input validation mechanisms for all external data input received via:

- 1033 • COM.Local;
- 1034 • COM.Adjacent; and
- 1035 • COM.Public.

1036 **EXAMPLE:** If an application expects the input to be an email address, any input that does not conform to the
1037 format of an e-mail address will be rejected.

1038 **NOTE 1:** The specific pattern to accept external data input depends amongst others on the manner the external data
1039 input is intended to be processed. This means that an acceptance pattern for broad purposes (such as
1040 administration via a "Secure Shell") is typically less specific than an acceptance pattern for a specific
1041 purpose (such as a measurement value of a specific format to be stored).

1042 **NOTE 2:** Typically the validation of different parts of the input will happen at different layers. Network layer of the
1043 operating system verify only information relevant to the network. An application verifies only input that
1044 is relevant to that application.

1045 **5.1.9.2 [LAS-INSAN] Sanitization of external data input**

1046 The SHGPVA shall use input sanitization mechanisms at application layer before using external data input, where the
1047 validation of external data input cannot prevent potential incidents triggered by the external data input.

1048 **EXAMPLE:** If external data input is amongst others intended to be stored via a database service, escape
1049 characters and other database service specific commands (defined by a corresponding function
1050 specific pattern) are removed from the external data input, before it is processed by the database
1051 service.

1052 **5.1.9.3 [LAS-PHY-INF] Only necessary physical interfaces**

1053 hardware architectural components shall only provide physical interfaces, that are necessary for the SHGPVA's
1054 intended purpose.

1055 **5.1.9.4 [LAS-LOGIC-INF] Only necessary logical interfaces active by default**

1056 The SHGPVA shall by default only provide logical interfaces, that are necessary for its intended purpose.

1057 **5.1.9.5 [LAS-APP] Only necessary apps by default**

1058 The SHGPVA shall by default only provide installed application software, that are necessary for its intended purpose.

1059 5.1.9.6 [LAS-SBOOT] Secure boot

1060 Where at least one function, whose use can cause harm with IMP.FH.High is provided by the SHGPVA and the
 1061 SHGPVA includes hardware architectural components, the hardware architectural components shall use a bootloader
 1062 function that only executes core software at startup, whose integrity and authenticity is verified.

1063 NOTE: The requirement corresponds to the verified boot capability in ETSI EN 304 623 vx.x.x [i.5]

1064 5.1.10 Logging and monitoring mechanisms

1065 5.1.10.1 [LOG-LOW] Events to log for low risk SHGPVA

1066 Where the SHGPVA has a function, whose use can cause harm of impact class low as its highest function impact class,
 1067 the SHGPVA shall support logging mechanisms to create audit events for every:

- 1068 • change of configuration affecting core software;
- 1069 • starts, shutdowns or other changes of operational states of core software;
- 1070 • errors of the core software;
- 1071 • capturing of audio or video data by an architectural component;
- 1072 • storage of captured audio or video data, or data derived thereof.

1073 5.1.10.2 [LOG-MEDIUM] Events to log for medium risk SHGPVA

1074 Where the SHGPVA has a function, whose use can cause harm of impact class medium as its highest function impact
 1075 class, the SHGPVA shall use logging mechanisms to create audit events for every:

- 1076 • unsuccessful authentication attempt;
- 1077 • change of configuration affecting core software;
- 1078 • starts, shutdowns or other changes of operational states of core software;
- 1079 • errors of the core software;
- 1080 • unsuccessful attempt of an identity to gain additional privileges;
- 1081 • unsuccessful attempt of an identity to access a data asset or function asset ;
- 1082 • capturing of audio or video data by an architectural component;
- 1083 • transmission of captured audio or video data, or data derived thereof;
- 1084 • storage of captured audio or video data, or data derived thereof.

1085 5.1.10.3 [LOG-HIGH] Events to log for high risk SHGPVA

1086 Where the SHGPVA has a function, whose use can cause harm of impact class high as its highest function impact class,
 1087 the SHGPVA shall use logging mechanisms to create audit events for every:

- 1088 • every authentication attempt;
- 1089 • change of configuration affecting core software;
- 1090 • starts, shutdowns or other changes of operational states of core software;
- 1091 • change of configuration affecting application software whom realize function, whose use can cause harm of
 1092 impact class high;
- 1093 • starts, shutdowns or other changes of operational states of application software whom realize function, whose
 1094 use can cause harm of impact class high;

- 1095 • errors of the core software;
- 1096 • errors of the application software whom realize function, whose use can cause harm of impact class high;
- 1097 • every attempt of an identity to gain additional privileges;
- 1098 • every attempt of an identity to access a data asset or function asset ;
- 1099 • capturing of audio or video data by an architectural component;
- 1100 • transmission of captured audio or video data, or data derived thereof;
- 1101 • storage of captured audio or video data, or data derived thereof.

1102 5.1.10.4 [LOG-TIME] Timestamps for logs

1103 Where the SHGPVA does not has a function, whose use can cause harm of impact class high, the SHGPVA shall use at
1104 least a time service or function to include a timestamp in every audit event, created by the SHGPVA.

1105 5.1.10.5 [LOG-TIME-HIGH] Real-Timestamps for logs

1106 Where the SHGPVA has a function, whose use can cause harm of impact class high as its highest function impact class,
1107 the SHGPVA shall use a real-time service or clock to include a real-time timestamp in every audit event, created by the
1108 SHGPVA.

1109 5.1.10.6 [LOG-STORAGE] Persistently store logfiles

1110 Where the SHGPVA has a function, whose use can cause harm of impact class medium or higher as its highest function
1111 impact class, the SHGPVA shall use integrity protecting secure storage mechanisms to store every audit event created
1112 by the SHGPVA persistently.

1113 5.1.10.7 [LOG-BACKUP] Backup of logfiles

1114 Where the SHGPVA has a function, whose use can cause harm of impact class high as its highest function impact class,
1115 the SHGPVA shall automatically backup its audit events to another device or another part of the SHGPVA that is in
1116 another physical location.

1117 5.1.10.8 [LOG-USER-ACC] User access to logs concerning their privacy.

1118 Where the SHGPVA is required to create audit events for any:

- 1119 • unsuccessful authentication attempt;
- 1120 • capturing of audio or video data by an architectural component;
- 1121 • transmission of captured audio or video data, or data derived thereof;
- 1122 • storage of captured audio or video data, or data derived thereof,

1123 the SHGPVA shall provide access for any user, to the logs of these events, which affect the privacy of this user.

1124 EXAMPLE: An overview of every time a voice controlled VAF processed a voice input command is stored in a
1125 cloud RDPS and accessible to all users of the SHGPVA.

1126 NOTE: These logs typically contain timestamps of these events and may include further personal data like e.g.,
1127 recorded audio, pictures, executed commands. These have than to be protected according to their,
1128 e.g. confidentiality impact class.

1129 5.1.11 Deletion mechanisms

1130 5.1.11.1 [DLM-PERM] Permanent removal of user-related data

1131 The SHGPVA shall provide at least one deletion mechanism that:

- 1132 • allows a user to permanently remove its user-related data, user-installed applications, including subsets of
1133 those; and
- 1134 • is easy to use.

1135 NOTE: This requirement differs mainly from [SDC-FRM] as [DLM-PERM] allows to delete single data assets.

1136 5.1.12 Other product's technical requirements specifications

1137 5.1.12.1 [USERNOT-NOSECFUC] User notifications on not available security 1138 functions

1139 The SHGPVA shall notify a user when security functions that are supposed to be used or supported by the SHGPVA
1140 are not available.

1141 5.1.12.2 [USERNOT-SECREL] Language and representation for security-related user 1142 notifications

1143 Where the SHGPVA is intended to be installed or maintained by a consumer for private usage, the SHGPVA shall use
1144 user notification mechanisms for security-related notifications that:

- 1145 • use a language that is clear, understandable, intelligible, legible and can be easily understood by users for
1146 security-related notifications; and
- 1147 • clearly distinguish the representation of security-related notifications from other notifications.

1148 5.1.12.3 [GUI-SECCONF] Visual representation of security-related configuration via 1149 GUIs

1150 Where the SHGPVA is intended to be installed or maintained by a consumer for private usage, and the SHGPVA
1151 provides a GUI for security-related configuration functionality, the SHGPVA shall ensure that those GUIs:

- 1152 • clearly distinguish security-related configuration options visually from other configuration options; and
- 1153 • clearly communicate the security-related consequences of changing each security-related configuration option
1154 in a language that is clear, understandable, intelligible, legible and can be easily understood by users; and
- 1155 • clearly highlight visually when changes to security-related configuration are made by a user.

1156 5.1.12.4 [CRY-SOTA] State-of-the-art cryptography

1157 The SHGPVA shall by default only use cryptographic algorithms for cryptographic functions that are

- 1158 • listed in Agreed Cryptographic Mechanisms [2]; or
- 1159 • suitable for the corresponding use.

1160 5.1.12.5 [CRY-CCK-PRE-LEN] Key size of preinstalled confidential cryptographic 1161 keys

1162 The SHGPVA shall only provide preinstalled confidential cryptographic keys of key sizes that are

- 1163 • listed in Agreed Cryptographic Mechanisms [2]; or
- 1164 • provide a minimum security strength of 112 bits.

1165 5.1.12.6 [CRY-CCK-GEN] Default key size of generated confidential cryptographic 1166 keys

1167 The SHGPVA shall by default only generate confidential cryptographic keys of key sizes that are

- 1168 • listed in Agreed Cryptographic Mechanisms [2]; or provide a minimum security strength of 112 bits.

1169 5.1.12.7 [CRY-PW-PRE-COM] Complexity of preinstalled passwords

1170 The SHGPVA shall only provide preinstalled passwords:

- 1171 • that meet the minimal recommended password complexity $C_{\{PW,min\}}$ determined by the corresponding
- 1172 authentication mechanisms' usage according to table 3, and
- 1173 • that are either
 - 1174 - individual per SHGPVA and not derivable via public available information or
 - 1175 - random per SHGPVA.

1176 5.1.12.8 [CRY-PW-GEN-COM] Default complexity of generated passwords

1177 The SHGPVA shall by default only generate passwords:

1178 of minimal recommended password complexity $C_{\{PW,min\}}$ determined by the corresponding authentication

1179 mechanisms' usage according to table 3 and that are random.

1180 5.1.12.9 [CRY-PW-USR-COM] Recommended complexity of user chosen passwords

1181 The SHGPVA shall only use user chosen passwords of minimal recommended password complexity $C_{\{PW,min\}}$

1182 determined by the corresponding authentication mechanisms' usage according table 3, except for user chosen passwords

1183 where the user explicitly confirms their usage after a warning by the SHGPVA.

1184 5.2 Requirements specifications for vulnerability handling

1185 activities related to the product

1186 The requirements specified in CEN/CLC JT013090:2026 (CEN/CLC prEN 40000-1-3) [1] shall be fulfilled for the

1187 SHGPVA.

1188 6 Assessing for compliance with requirements

1189 6.1 Assessing for compliance with product's technical

1190 requirements specifications

1191 6.1.1 General

1192 In order to assess the compliance with the requirements listed in clause 5.1 of the present document, the assessment

1193 procedures described in clause 6.1 are to be followed. When performing assessments, the distribution of security

1194 functions (see clause 4.5) are to be considered, including whether the product provides security functions itself,

1195 demands them from other products with digital elements within its context, or supplies them to other products with

1196 digital elements.

1197 If there are already existing evidences (e.g. provided by manufacturers of components that are integrated in the

1198 SHGPVA) that:

- 1199 • are covering the same assessment activities as described in clause 6.1, and
- 1200 • are valid for the moment of the assessment to be performed under clause 6.1,

1201 those existing evidences can be used for the "assignment of verdict" and as "supporting evidence".

1202 6.1.2 Known exploitable vulnerabilities

1203 6.1.2.1 Assessment criteria for [NKEV-SUM-SUPPORT]

1204 **Assessment objective:**

1205 The assessment covers:

- 1206 • a conceptual assessment of [NKEV-SUM-SUPPORT],
- 1207 • a functional completeness assessment on the SHGPVA's capabilities that are addressed by
- 1208 [NKEV-SUM-SUPPORT]
- 1209 • a functional sufficiency assessment of each software update mechanism used by the SHGPVA to fulfil
- 1210 [NKEV-SUM-SUPPORT]

1211 based on the default configuration required by clause [5.1.2](#).

1212 **Assessment preparation:**

1213 The following documentation for the SHGPVA shall be complete:

- 1214 • a list of all software architectural components of the SHPSF,
- 1215 • a list of software architectural components declared immutable, including technical justification,
- 1216 • documentation describing all supported software update mechanisms, including:
 - 1217 - their scope, and
 - 1218 - interfaces through which updates can be invoked.

1219 The following test setups shall be prepared:

- 1220 • a test setup that allows to identify software update mechanisms on a sample SHGPVA 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 SHGPVA's conformity to [NKEV-SUM-SUPPORT] shall be validated based on the documentation.
- 1226 • The correctness and completeness of the documentation shall be verified by:
 - 1227 - inspecting the SHGPVA to identify software architectural components, e.g. by generating SBOMs
 - 1228 - 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 SHGPVA's conformity with [NKEV-SUM-SUPPORT]; 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 6.1.2.2 Assessment criteria for [NKEV-SUM-PROVIDE]

1246 **Assessment objective:**

1247 The assessment covers:

- 1248 • a conceptual assessment of [NKEV-SUM-PROVIDE],
- 1249 • a functional completeness assessment on the capabilities of the SHGPVA's architectural components that are
- 1250 addressed by [NKEV-SUM-PROVIDE]
- 1251 • a functional sufficiency assessment of each software update mechanism provided by the SHGPVA's
- 1252 architectural components to fulfil [NKEV-SUM-PROVIDE]

1253 based on the default configuration required by clause [5.1.2](#).

1254 **Assessment preparation:**

1255 The following documentation for the SHGPVA shall be complete:

- 1256 • a list of all architectural components of the SHGPVA that include core software,
- 1257 • a list of architectural components declared immutable, including technical justification,
- 1258 • documentation describing all provided software update mechanisms, including:
 - 1259 - their scope, and
 - 1260 - interfaces through which updates can be invoked.

1261 The following test setups shall be prepared:

- 1262 • a test setup that allows to identify software update mechanisms on sample architectural components of the
- 1263 SHGPVA in default configuration;
- 1264 • for each software update mechanism, a test setup that allows to perform an update over that software update
- 1265 mechanism

1266 **Assessment activities:**

1267 The following activities shall be performed:

- 1268 • The SHGPVA's conformity to [NKEV-SUM-PROVIDE] shall be validated based on the documentation.
- 1269 • The correctness and completeness of the documentation shall be verified by:
 - 1270 - inspecting the architectural components of the SHGPVA that include core software and
 - 1271 - checking whether each identified component is associated with a documented update path.
- 1272 • For each software update mechanism, its correct implementation shall be verified by:
 - 1273 - installing an update over this software update mechanism to update a software architectural component
 - 1274 and
 - 1275 - checking whether the software has changed to the updated software.

1276 **Assignment of verdict:**

1277 The verdict PASS shall be assigned if:

- 1278 • the documentation indicates the SHGPVA's conformity with [NKEV-SUM-PROVIDE]; and
- 1279 • the verification of the correctness and completeness of the documentation was successful; and
- 1280 • the verification of the correct implementation of each software update mechanism was successful.

1281 The verdict FAIL shall be assigned otherwise.

1282 **Supporting Evidence:**

- 1283 • records of the validation of the documentation
- 1284 • descriptions of the performed tests and records of performed tests to verify the correctness and completeness
1285 of the documentation
- 1286 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each
1287 software update mechanism

1288 **6.1.2.3 Assessment criteria for [NKEV-SUM-AUTO]**

1289 **Assessment objective:**

1290 The assessment covers:

- 1291 • a conceptual assessment of [NKEV-SUM-AUTO],
- 1292 • a functional sufficiency assessment of each software update mechanism used by the SHPSF to fulfil
1293 [NKEV-SUM-AUTO]

1294 based on the default configuration required by clause [5.1.2](#).

1295 **Assessment preparation:**

1296 The following documentation for the SHGPVA shall be complete:

- 1297 • documentation describing all supported software update mechanism, including:
 - 1298 - their scope,
 - 1299 - interfaces through which updates can be invoked, and
 - 1300 - their capability to perform automatic updates

1301 The following test setups shall be prepared:

- 1302 • for each software update mechanism, a test setup that ensures internet-connectivity and that allows to perform
1303 an automatic update over that software update mechanism

1304 **Assessment activities:**

1305 The following activities shall be performed:

- 1306 • The SHGPVA's conformity to [NKEV-SUM-AUTO] shall be validated based on the documentation.
- 1307 • For each software update mechanism, its correct implementation shall be verified by:
 - 1308 - installing an automatic update with internet connection over this software update mechanism to update a
1309 software architectural component,
 - 1310 - checking whether the product performs the automatic update without human intervention at the product
1311 or via scheduling the installation under human approval or via triggering the installation under human
1312 approval, and
 - 1313 - checking whether the software version has been updated to a new version.

1314 **Assignment of verdict:**

1315 The verdict PASS shall be assigned if:

- 1316 • the documentation indicates the SHGPVA's conformity with [NKEV-SUM-AUTO] and
- 1317 • the verification of the correct implementation of each software update mechanism was successful.

1318 The verdict FAIL shall be assigned otherwise.

1319 **Supporting Evidence:**

- 1320 • records of the validation of the documentation
- 1321 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each
- 1322 software update mechanism

1323 **6.1.2.4 Assessment criteria for [NKEV-SUM-NOTIF]**

1324 **Assessment objective:**

1325 The assessment covers:

- 1326 • a conceptual assessment of [NKEV-SUM-NOTIF],
- 1327 • a functional completeness assessment on the SHGPVA's capabilities that are addressed by
- 1328 [NKEV-SUM-NOTIF]
- 1329 • a functional sufficiency assessment of each software update notification mechanism used by the SHGPVA to
- 1330 fulfil [NKEV-SUM-NOTIF]

1331 based on the default configuration required by clause [5.1.2](#).

1332 **Assessment preparation:**

1333 The following documentation for the SHGPVA shall be complete:

- 1334 • documentation describing all supported software update notification mechanisms, including:
 - 1335 - how the software update notification is performed, and
 - 1336 - to what extent this software update notification is automated.

1337 The following test setups shall be prepared:

- 1338 • a test setup that allows to identify software update notification mechanisms on a sample SHGPVA in default
- 1339 configuration;
- 1340 • for each software update notification mechanism, a test setup that allows to make software updates available
- 1341 and therefore to trigger the notification

1342 **Assessment activities:**

1343 The following activities shall be performed:

- 1344 • The SHGPVA's conformity to [NKEV-SUM-NOTIF] shall be validated based on the documentation.
- 1345 • The correctness and completeness of the documentation shall be verified by:
 - 1346 - inspecting the SHGPVA to identify software update notification mechanisms.
- 1347 • For each software update notification mechanism, its correct implementation shall be verified by:
 - 1348 - making a software update available at the source holding security updates and

- 1349 - checking whether the software update notification mechanism automatically notifies the SHGPVA's
1350 users that an update of its software is available

1351 **Assignment of verdict:**

1352 The verdict PASS shall be assigned if:

- 1353 • the documentation indicates the SHGPVA's conformity with [NKEV-SUM-NOTIF]; and
- 1354 • the verification of the correctness and completeness of the documentation was successful; and
- 1355 • the verification of the correct implementation of each software update notification mechanism was successful.

1356 The verdict FAIL shall be assigned otherwise.

1357 **Supporting Evidence:**

- 1358 • records of the validation of the documentation
- 1359 • descriptions of the performed tests and records of performed tests to verify the correctness and completeness
1360 of the documentation
- 1361 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each
1362 software update notification mechanism

1363 **6.1.3 Default configuration**

1364 **6.1.3.1 Assessment criteria for [SDC-AUM-FH]**

1365 **Assessment objective:**

1366 The assessment covers:

- 1367 • a conceptual assessment of [SDC-AUM-FH];
- 1368 • a functional completeness assessment on the SHGPVA capabilities that are addressed by [SDC-AUM-FH];

1369 based on the factory default state.

1370 NOTE: A functional sufficiency assessment of each authentication mechanism used by the SHGPVA to fulfil
1371 [SDC-AUM-FH] is addressed by the assessment of [AUM-FH].

1372 **Assessment preparation:**

1373 The following documentation for the SHGPVA shall be complete:

- 1374 • a list of SHGPVA's functions whose use can cause harm that are enabled in the factory default state or can be
1375 activated during initialisation.
- 1376 - the physical operational environment of the architectural component that performs the function;
- 1377 - for each of the function's trigger input possibilities:
 - 1378 ▪ the interface and communication type;
 - 1379 ▪ a list of corresponding authentication mechanisms including:
 - 1380 • the authentication mechanisms' strength;

1381 NOTE: This documentation is a subset of the documentation required for the assessment of [AUM-FH]

1382 The following test setups shall be prepared:

- 1383 • a test setup for identifying functions, their trigger input possibilities and corresponding authentication
1384 mechanisms based on a sample SHGPVA in factory default state and after initialisation

1385 **Assessment activities:**

- 1386 • The SHGPVA's conformity to [SDC-AUM-FH] shall be validated based on the documentation.
- 1387 • The correctness and completeness of the documentation shall be verified by:
- 1388 - inspecting the SHGPVA in factory default state; and
- 1389 - (if functions whose use can cause harm can be configured during initialisation) performing the
- 1390 initialisation without providing explicit confirmation of configurations deviating from the minimal
- 1391 required authentication strength determined by table 3 and inspecting the SHGPVA after initialisation.

1392 **Assignment of verdict:**

1393 The verdict PASS shall be assigned if:

- 1394 • the documentation indicates the SHGPVA's conformity to [SDC-AUM-FH]; and
- 1395 • the verification of the correctness and completeness of the documentation was successful

1396 The verdict FAIL shall be assigned otherwise.

1397 **Supporting Evidence:**

- 1398 • records of the validation of the documentation;
- 1399 • descriptions of the performed tests and records of performed tests to verify the correctness and completeness
- 1400 of the documentation.

1401 **6.1.3.2 Assessment criteria for [SDC-FRM]**

1402 **Assessment objective:**

1403 The assessment functionally determines whether all user-related data, installed applications, and configurations

1404 deviating from the default state are erased after using the factory reset mechanism.

1405 **Assessment preparation:**

- 1406 • Documentation on how the factory reset mechanism can be accessed.
- 1407 • The SHGPVA shall be set up and some configuration changes shall be created and persistently stored.
- 1408 • Where the SHGPVA supports the storage of user-related data, some user-related data shall be created and
- 1409 persistently stored on the SHGPVA.
- 1410 • Where the SHGPVA supports the installation of applications, some common application for the SHGPVA
- 1411 shall be installed.

1412 NOTE: User-related data also encompasses cryptographic keys, e.g. Wi-Fi® passwords, certificates.

1413 **Assessment activities:**

- 1414 • An authorised entity shall start the factory reset mechanism.
- 1415 • The erasure of user-related data, applications and configurations shall be validated:
- 1416 - The restoration of the device settings to their default state shall be validated.
- 1417 • Attempts to access any previous user accounts or data shall be made.

1418 **Assignment of verdict:**

1419 The verdict PASS shall be assigned when all user-related data, installed applications, and configurations deviating from

1420 the default state are erased

1421 The verdict FAIL shall be assigned otherwise.

1422 **Supporting Evidence:**

- 1423 • Description of the performed test
- 1424 • All test records of the performed test

1425 **6.1.4 Authentication and access control mechanisms**

1426 **6.1.4.1 Assessment criteria for [ACM-FH]**

1427 **Assessment objective:**

1428 The assessment covers:

- 1429 • a conceptual assessment of [ACM-FH];
- 1430 • a functional completeness assessment on the SHGPVA capabilities that are addressed by [ACM-FH];
- 1431 • a functional sufficiency assessment of each access control mechanism used by the SHGPVA to fulfil
- 1432 [ACM-FH]

1433 based on the default configuration required by clause [5.1.2](#).

1434 **Assessment preparation:**

1435 The following documentation for the SHGPVA shall be complete:

- 1436 • a list of SHGPVA'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 access control mechanisms including their default authorization policy.

1443 The following test setups shall be prepared:

- 1444 • a test setup for identifying functions, their trigger input possibilities and corresponding access control
- 1445 mechanisms based on a sample SHGPVA in default configuration;
- 1446 • for each access control mechanism, a test setup that allows privilege escalation attacks from authenticated
- 1447 entities and unauthorized access attempts of unauthenticated entities.

1448 **Assessment activities:**

- 1449 • The SHGPVA's conformity to [ACM-FH] shall be validated based on the documentation.
- 1450 • The correctness and completeness of the documentation shall be verified by:
 - 1451 - an inspection of the SHGPVA for functions and related access control mechanisms that are accessible via
 - 1452 physical human interfaces;
 - 1453 - a scan of the SHGPVA for functions and related access control mechanisms that are accessible via
 - 1454 logical interfaces.
 - 1455 • For each access control mechanism, its correct implementation shall be verified based on attempts to violate
 - 1456 the authorization policy by:
 - 1457 - privilege escalation of authenticated entities based on the default authorization policy;

1458 - unauthorized usage of function, whose use can cause harm by unauthenticated entities based on the
1459 default authorization policy.

1460 **Assignment of verdict:**

1461 The verdict PASS shall be assigned if:

- 1462 • the documentation indicates the SHGPVA's conformity to [ACM-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 access control 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 access control mechanism

1472 **6.1.4.2 Assessment criteria for [AUM-FH]**

1473 **Assessment objective:**

1474 The assessment covers:

- 1475 • a conceptual assessment of [AUM-FH];
- 1476 • a functional completeness assessment on the SHGPVA capabilities that are addressed by [AUM-FH];
- 1477 • a functional sufficiency assessment of each authentication mechanism used by the SHGPVA to fulfil
1478 [AUM-FH]

1479 based on the default configuration required by clause [5.1.2](#).

1480 **Assessment preparation:**

1481 The following documentation for the SHGPVA shall be complete:

- 1482 • a list of SHGPVA's functions whose use can cause harm
- 1483 • for each function, whose use can cause harm:
 - 1484 - its impact class impact class for function, whose use can cause harm;
 - 1485 - the physical operational environment of the architectural component that performs the function;
 - 1486 - for each of the function's trigger input possibilities:
 - 1487 ▪ the interface and communication type;
 - 1488 ▪ a list of corresponding authentication mechanisms including:
 - 1489 • the authentication mechanisms' strength;
 - 1490 • the type of authentication factors.

1491 The following test setups shall be prepared:

- 1492 • a test setup for identifying functions, their trigger input possibilities and corresponding authentication
1493 mechanisms based on a sample SHGPVA in default configuration;

- 1494 • for each authentication mechanism, a test setup defined by the test cases provided in clause [E.1](#) according to
1495 the needs determined by its strength and the type of its authentication factors.

1496 **Assessment activities:**

- 1497 • The SHGPVA's conformity to [AUM-FH] shall be validated based on the documentation.
- 1498 • The correctness and completeness of the documentation shall be verified by:
- 1499 - an inspection of the SHGPVA for functions and related authentication mechanisms that are accessible
1500 via physical human interfaces;
- 1501 - a scan of the SHGPVA for functions and related authentication mechanisms that are accessible via
1502 logical interfaces.
- 1503 • For each authentication mechanism, its correct implementation shall be verified based on the test cases
1504 provided in clause [E.1](#) according to the needs determined by its strength and the type of its authentication
1505 factors.

1506 **Assignment of verdict:**

1507 The verdict PASS shall be assigned if:

- 1508 • the documentation indicates the SHGPVA's conformity to [AUM-FH]; and
- 1509 • the verification of the correctness and completeness of the documentation was successful; and
- 1510 • the verification of the correct implementation of each authentication mechanism was successful.

1511 The verdict FAIL shall be assigned otherwise.

1512 **Supporting Evidence:**

- 1513 • records of the validation of the documentation;
- 1514 • descriptions of the performed tests and records of performed tests to verify the correctness and completeness
1515 of the documentation;
- 1516 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each
1517 authentication mechanism.

1518 **6.1.4.3 Assessment criteria for [AUTHZ-LP]**

1519 **Assessment objective:**

1520 The assessment covers:

- 1521 • a conceptual assessment of [AUTHZ-LP].

1522 based on the default configuration required by clause [5.1.2](#)

1523 **Assessment preparation:**

1524 The following documentation for the SHGPVA shall be complete:

- 1525 • a description of the authorization policies in default configuration including:
- 1526 - a list of granted permissions for entities on function, whose use can cause harm and
- 1527 - for each granted permission, a justification that it is necessary for the intended purpose.

1528 **Assessment activities:**

- 1529 • The SHGPVA's conformity to [AUTHZ-LP] shall be validated based on the documentation.

1530 **Assignment of verdict:**

1531 The verdict PASS shall be assigned if:

- 1532 • the documentation indicates the SHGPVA's conformity to [AUTHZ-LP].

1533 The verdict FAIL shall be assigned otherwise.

1534 **Supporting Evidence:**

- 1535 • records of the validation of the documentation

1536 **6.1.4.4 Assessment criteria for [AUTHZ-R]**

1537 **Assessment objective:**

1538 The assessment covers:

- 1539 • a functional sufficiency assessment to ensure the SHGPVA supports revocation of any granted permissions.

1540 **Assessment preparation:**

1541 The following documentation for the SHGPVA shall be complete:

- 1542 • a list of mechanisms to grant permissions for entities on function, whose use can cause harm.

1543 The following test setups shall be prepared:

- 1544 • for each mechanism to grant permissions, a test setup for granting and revoking permissions for entities on
1545 function, whose use can cause harm.

1546 **Assessment activities:**

- 1547 • For each mechanism to grant permissions, the revocability of grantable permissions shall be verified by:
 - 1548 - granting permissions to an entity;
 - 1549 - revoking the permissions; and
 - 1550 - attempting use permissions after revocation.

1551 **Assignment of verdict:**

1552 The verdict PASS shall be assigned if:

- 1553 • for each mechanism to grant permissions, access is denied after revocation.

1554 The verdict FAIL shall be assigned otherwise.

1555 **Supporting Evidence:**

- 1556 • descriptions of the performed tests and records of performed tests to verify the correct implementation of
1557 [AUTHZ-R].

1558 **6.1.5 Integrity protection**

1559 **6.1.6 Confidentiality protection**

1560 **6.1.7 Data minimization**

1561 **6.1.7.1 Assessment criteria for [DMIN-DJST]**

1562 **Assessment objective:**

1563 The assessment covers:

- 1564 • a conceptual assessment of Documented justification of processed data

1565 **Assessment preparation:**

1566 The following documentation for the SHGPVA shall be complete:

- 1567 • a list of all data assets processed by the SHGPVA whose impact class for confidential SHGPVA data is
1568 IMP.CONF.Low or higher;
- 1569 • for each documented confidential data asset, the associated rationale for its necessity explaining why its
1570 processing is necessary for the intended purpose of the SHGPVA.

1571 **Assessment activities:**

- 1572 • The SHGPVA's conformity to [DMIN-DJST] shall be validated based on the documentation.

1573 **Assignment of verdict:**

1574 The verdict PASS shall be assigned if:

- 1575 • the documentation indicates the SHGPVA's conformity to [DMIN-DJST];

1576 Otherwise, the verdict FAIL shall be assigned.

1577 **Supporting Evidence:**

- 1578 • records of the validation of the documentation;

1579 6.1.8 Availability protection

1580 6.1.8.1 Assessment criteria for [AVAI-TIME-RECO-POW]

1581 **Assessment objective:**

1582 The assessment covers:

- 1583 • a functional sufficiency assessment of the recovery function interaction with each power supply used by the
1584 SHGPVA's hardware architectural components to fulfil [AVAI-TIME-RECO-POW]

1585 based on the default configuration required by clause [5.1.2](#).

1586 **Assessment preparation:**

1587 The following documentation for the SHGPVA shall be complete:

- 1588 • a list of all SHGPVA's hardware architectural components:
- 1589 • for each SHGPVA's hardware architectural component:
 - 1590 - a list of all power supplies
 - 1591 - for each power supply:
 - 1592 ▪ a description whether the power supply can power the hardware architectural component alone
 - 1593 - a list of all functionalities of the SHGPVA that need communication involving the hardware architectural
1594 component:
 - 1595 ▪ for each of these functionalities:
 - 1596 • a list of interfaces of the SHGPVA, where the connection status of the necessary
1597 communication channels can be read; OR
 - 1598 • parameters of the necessary communication channels of the hardware architectural
1599 components in order to externally observe if the connection is active

1640 **Supporting Evidence:**

- 1641 • descriptions of the performed tests and records of performed tests

1642 **6.1.8.2 Assessment criteria for [AVAI-TIME-NETW]**

1643 **Assessment objective:**

1644 The assessment covers:

- 1645 • a conceptual assessment of [AVAI-TIME-NETW];
- 1646 • a functional completeness assessment on the SHGPVA capabilities that are addressed by
1647 [AVAI-TIME-NETW];
- 1648 • a functional sufficiency assessment of each time sensitive function without the need of network connectivity to
1649 operate used by the SHGPVA to fulfil [AVAI-TIME-NETW]

1650 based on the default configuration required by clause [5.1.2](#).

1651 **Assessment preparation:**

1652 The following documentation for the SHGPVA shall be complete:

- 1653 • a list of all time sensitive function of the SHGPVA:
- 1654 • for each time sensitive function:
- 1655 - description of the functionalities realised or supported by this function
- 1656 - list of interfaces necessary for the operation of this function
- 1657 ▪ for each interface:
- 1658 ▪ communication types of the interface
- 1659 • a list of interfaces of the SHGPVA, where the status of the architectural component's time sensitive function
1660 can be read
- 1661 - description how the status can be implied from the interface readings

1662 The following test setups shall be prepared:

- 1663 • the SHGPVA is set up in default configuration
- 1664 • a test setup to:
- 1665 - disconnect or disable the public communication of the SHGPVA's architectural components
- 1666 - disconnect or disable the adjacent communication of the SHGPVA's architectural components
- 1667 - enable access to at least one interfaces of the SHGPVA, where the status of the SHGPVA's time sensitive
1668 function can be read

1669 **Assessment activities:**

1670 The following activities shall be performed:

- 1671 • verify the correctness and completeness of the documentation
- 1672 • repeat the following steps for communication types public communication, adjacent communication and both,
1673 depending on the communication type needed by the functions to be tested:
- 1674 - disconnect or disable the corresponding communication type of the SHGPVAs architectural component
- 1675 - wait at least 30 s

- 1676 - for each time sensitive function which does not need any interface with the corresponding
1677 communication type for its operation
- 1678 ▪ check whether the function is in operable status
- 1679 ▪ record the status of the function and the disconnected or disabled communication type
- 1680 - reconnect or enable the corresponding communication type

1681 **Assignment of verdict:**

1682 The verdict PASS shall be assigned if:

- 1683 • no indication, that the documentation is incorrect or incomplete, are found
- 1684 • all checked time sensitive functions are in operable state

1685 The verdict FAIL shall be assigned otherwise.

1686 **Supporting Evidence:**

- 1687 • descriptions of the performed tests and records of performed tests

1688 **6.1.8.3 Assessment criteria for [AVAI-TIME-RECO-NETW]**

1689 **Assessment objective:**

1690 The assessment covers:

- 1691 • a conceptual assessment of [AVAI-TIME-RECO-NETW]
- 1692 • a functional completeness assessment on the SHGPVA capabilities that are addressed by
1693 [AVAI-TIME-RECO-NETW]
- 1694 • a functional sufficiency assessment of the SHGPVAs architectural components recovery after loss of network
1695 connection, to fulfil [AVAI-TIME-RECO-NETW]

1696 based on the default configuration required by clause [5.1.2](#).

1697 **Assessment preparation:**

1698 The following documentation for the SHGPVA shall be complete:

- 1699 • a list of all functions of the SHGPVA that need communication involving the architectural component
- 1700 - for each of these functions:
- 1701 ▪ list of interfaces involving the architectural component and are necessary for the operation of this
1702 function:
- 1703 • for each interface:
- 1704 ○ communication types of the interface
- 1705 - a list of interfaces of the SHGPVA, where the connection status of the necessary communication
1706 channels can be read; OR
- 1707 - parameters of the necessary communication channel of the architectural component in order to externally
1708 observe if the connection is active

1709 The following test setups shall be prepared:

- 1710 • the SHGPVA is set up in default configuration
- 1711 • a test setup to:

- 1712 - disconnect or disable the public communication of the SHGPVAs architectural component
- 1713 - disconnect or disable the adjacent communication of the SHGPVAs architectural component
- 1714 - enable access to at least one interfaces of the SHGPVA, where the connection status the necessary
1715 interfaces involving the architectural component and are necessary for the operation of these functions
1716 can be read; OR
- 1717 - if the connection status for all necessary interfaces involving the architectural component and are
1718 necessary for the operation of these functions cannot be read from the SHGPVA:
- 1719 ▪ monitor whether all necessary interfaces involving the architectural component and are necessary
1720 for the operation of these functions

1721 **Assessment activities:**

1722 The following activities shall be performed:

- 1723 • verify the correctness and completeness of the documentation by:
- 1724 - check for undocumented interfaces
- 1725 • repeat the following steps for communication types public communication, adjacent communication and both
1726 at the same time:
- 1727 - disconnect or disable the corresponding communication type of the SHGPVAs architectural component
- 1728 - wait at least 60s
- 1729 - reconnect or enable the corresponding communication type
- 1730 - record the corresponding communication type
- 1731 - for each documented function:
- 1732 ▪ monitor the operational status of the function
- 1733 ▪ for each interface necessary for the operation of this function:
- 1734 • monitor the connection status
- 1735 • record the time relative to the reconnection or enabling of the corresponding
1736 communication type, after which the SHGPVA indicates, that the interface is
1737 reconnected; OR
- 1738 • record the time relative to the reconnection or enabling of the corresponding
1739 communication type, after which the interface was active at least once, and there is
1740 no indication that the SHGPVA has not resumed operation

1741 **Assignment of verdict:**

1742 The verdict PASS shall be assigned if:

- 1743 • no indication, that the documentation is incorrect or incomplete, are found; and
- 1744 • the SHGPVA signals resume of operations and establishment of all necessary communication channels within
1745 one hour; OR
- 1746 • all necessary communication channels of the architectural component were active at least once, and there is no
1747 indication that the SHGPVA has not resumed operation within one hour
- 1748 • The verdict FAIL shall be assigned otherwise.

1749 **Supporting Evidence:**

- 1750 • descriptions of the performed tests and records of performed tests

1751 **6.1.8.4 Assessment criteria for [AVAI-TIME-OUTA-NOT]**

1752 **Assessment objective:**

1753 The assessment covers:

- 1754 • a conceptual assessment of [AVAI-TIME-OUTA-NOT]
- 1755 • a functional sufficiency assessment of the SHGPVAs notification in case of non-availability induced by
1756 network resource restrictions, to fulfil [AVAI-TIME-OUTA-NOT]
- 1757 • a functional sufficiency assessment of the SHGPVAs notification in case of non-availability induced by DOS,
1758 to fulfil [AVAI-TIME-PREV-NOT]

1759 based on the default configuration required by clause [5.1.2](#).

1760 **Assessment preparation:**

1761 The following documentation for the SHGPVA shall be complete:

- 1762 • description how the status of the SHGPVAs time sensitive functions can be read or deduced
- 1763 • a list of all time sensitive functions of the SHGPVA:
 - 1764 - for each of these functions:
 - 1765 ▪ the time sensitive availability impact class
 - 1766 ▪ whether the function needs network connectivity
- 1767 • CPU, memory, power and network resources available to the SHGPVA
- 1768 • demands on CPU, memory, power and network resources for workload consistent with the SHGPVAs
1769 intended purpose and reasonably foreseeable use
- 1770 • a list of all notification mechanisms of the SHGPVA:
 - 1771 - description how the notification mechanism can be configured

1772 The following test setups shall be prepared:

- 1773 • the SHGPVA is set up in default configuration
- 1774 • configure at least one notification mechanism
- 1775 • a test setup to:
 - 1776 - limit the network bandwidth between the SHGPVAs architectural component and the SHGPVAs RDPS
1777 to the internet
 - 1778 - induce a denial-of-service status on the SHGPVA causing increasing demand on processing resources
 - 1779 - receive notifications from the SHGPVA

1780 **Assessment activities:**

1781 The following activities shall be performed:

- 1782 • verify the correctness and completeness of the documentation
- 1783 • conceptually verify whether the documented notification mechanisms are suitable to send notifications in case
1784 of resource limitations
- 1785 • if at least on time sensitive function needs network connectivity:
 - 1786 - progressively lower the network bandwidth available to the SHGPVAs architectural component

- 1787 ▪ record any received notifications form the SHGPVA
- 1788 - progressively higher the intensity of requests to induce a denial-of-service status on the SHGPVA
- 1789 ▪ record any received notifications form the SHGPVA
- 1790 **Assignment of verdict:**
- 1791 The verdict PASS shall be assigned if:
- 1792 • no indication, that the documentation is incorrect or incomplete, are found; and
- 1793 • the SHGPVA sends notifications according to its configuration in case of non-availability of time sensitive
- 1794 function with IMP.AVAI.TIME.Medium or higher induced by DOS; or
- 1795 - no time sensitive function with IMP.AVAI.TIME.Medium or higher was non-availability due to DOS;
- 1796 and
- 1797 • the SHGPVA sends notifications according to its configuration in case of non-availability of time sensitive
- 1798 function with IMP.AVAI.TIME.Medium or higher induced by network bandwidth limitation; or
- 1799 - no time sensitive function with IMP.AVAI.TIME.Medium or higher was non-availability due to network
- 1800 bandwidth limitation.

1801 The verdict FAIL shall be assigned otherwise.

1802 **Supporting Evidence:**

- 1803 • descriptions of the performed tests and records of performed tests

1804 **6.1.8.5 Assessment criteria for [AVAI-TIME-PREV-NOT]**

1805 **Assessment objective:**

1806 The assessment covers:

- 1807 • a conceptual assessment of [AVAI-TIME-PREV-NOT]
- 1808 • a functional sufficiency assessment of the SHGPVAs notification in case of network resource restrictions, to
- 1809 fulfil [AVAI-TIME-PREV-NOT]
- 1810 • a functional sufficiency assessment of the SHGPVAs notification in case of DOS, to fulfil
- 1811 [AVAI-TIME-PREV-NOT]

1812 based on the default configuration required by clause [5.1.2](#).

1813 **Assessment preparation:**

1814 The following documentation for the SHGPVA shall be complete:

- 1815 • a list of all time sensitive functions of the SHGPVA:
- 1816 - for each of these functions:
- 1817 ▪ the time sensitive availability impact class
- 1818 ▪ whether the function needs network connectivity
- 1819 • CPU, memory, power and network resources available to the SHGPVA
- 1820 • demands on CPU, memory, power and network resources for workload consistent with the SHGPVAs
- 1821 intended purpose and reasonably foreseeable use
- 1822 • a list of all notification mechanisms of the SHGPVA:
- 1823 - description how the notification mechanism can be configured

1824 The following test setups shall be prepared:

- 1825 • the SHGPVA is set up in default configuration
- 1826 • configure at least one notification mechanism
- 1827 • a test setup to:
 - 1828 - read or deduced the status of the time sensitive functions from the SHGPVA
 - 1829 - limit the network bandwidth between the SHGPVAs architectural component and the SHGPVAs RDPS
 - 1830 to the internet
 - 1831 - induce a DOS status on the SHGPVA causing increasing demand on processing resources
 - 1832 - receive notifications from the SHGPVA

1833 **Assessment activities:**

1834 The following activities shall be performed:

- 1835 • verify the correctness and completeness of the documentation
- 1836 • conceptually verify whether the documented notification mechanisms are suitable to send notifications in case
- 1837 of resource limitations
- 1838 • if at least on time sensitive function needs network connectivity:
 - 1839 - progressively lower the network bandwidth available to the SHGPVAs architectural component
 - 1840 ▪ record any received notifications form the SHGPVA
 - 1841 - progressively higher the intensity of requests to induce a DOS status on the SHGPVA
 - 1842 ▪ record any received notifications form the SHGPVA

1843 **Assignment of verdict:**

1844 The verdict PASS shall be assigned if:

- 1845 • no indication, that the documentation is incorrect or incomplete, are found; and
- 1846 • the SHGPVA sends notifications according to its configuration in case of resource limitations induced by
- 1847 DOS; and
- 1848 • the SHGPVA sends notifications according to its configuration in case of network bandwidth limitation; or
 - 1849 - no time sensitive function with IMP.AVAI.TIME.High of the SHGPVA of the SHGPVA needs network
 - 1850 connectivity

1851 The verdict FAIL shall be assigned otherwise.

1852 **Supporting Evidence:**

- 1853 • descriptions of the performed tests and records of performed tests

1854 **6.1.8.6 Assessment criteria for [AVAI-TIME-NET-PRIO]**

1855 **Assessment objective:**

1856 The assessment covers:

- 1857 • a conceptual assessment of [AVAI-TIME-NET-PRIO]
- 1858 • a functional sufficiency assessment of the SHGPVAs resource prioritization in case of non-availability
- 1859 induced by network resource restrictions, to fulfil [AVAI-TIME-NET-PRIO]

1860 based on the default configuration required by clause [5.1.2](#).

1861 **Assessment preparation:**

1862 The following documentation for the SHGPVA shall be complete:

- 1863 • description how the status of the SHGPVAs time sensitive functions can be read or deduced
- 1864 • a list of all time sensitive functions of the SHGPVA:
 - 1865 - for each of these functions:
 - 1866 ▪ the time sensitive availability impact class
 - 1867 ▪ whether the function needs network connectivity
- 1868 • prioritization policy for the time sensitive functions of the SHGPVA in case of network resource conflict

1869 The following test setups shall be prepared:

- 1870 • the SHGPVA is set up in default configuration
- 1871 • a test setup to:
 - 1872 - read or deduced the status of the time sensitive functions from the SHGPVA
 - 1873 - limit the network bandwidth between the SHGPVAs architectural component and the SHGPVAs RDPS
 - 1874 to the internet

1875 **Assessment activities:**

1876 The following activities shall be performed:

- 1877 • verify the correctness and completeness of the documentation
- 1878 • conceptually verify the prioritization policy
- 1879 • progressively lower the network bandwidth available to the SHGPVAs architectural component
 - 1880 - record the status of every time sensitive function

1881 **Assignment of verdict:**

1882 The verdict PASS shall be assigned if:

- 1883 • no indication, that the documentation is incorrect or incomplete, are found; and
- 1884 • the prioritization policy is conceptually valid; and
- 1885 • the prioritization policy is represented by the status of every time sensitive function during network bandwidth
- 1886 limitation.

1887 The verdict FAIL shall be assigned otherwise.

1888 **Supporting Evidence:**

- 1889 • descriptions of the performed tests and records of performed tests

1890 **6.1.8.7 Assessment criteria for [AVAI-TIME-RES-PRIO]**

1891 **Assessment objective:**

1892 The assessment covers:

- 1893 • a conceptual assessment of [AVAI-TIME-RES-PRIO]

- 1894 • a functional sufficiency assessment of the SHGPVAs resource prioritization in case of non-availability
1895 induced by DOS, to fulfil [AVAI-TIME-RES-PRIO]

1896 based on the default configuration required by clause [5.1.2](#).

1897 **Assessment preparation:**

1898 The following documentation for the SHGPVA shall be complete:

- 1899 • description how the status of the SHGPVAs time sensitive functions can be read or deduced
- 1900 • a list of all time sensitive functions of the SHGPVA:
 - 1901 - for each of these functions:
 - 1902 ▪ the time sensitive availability impact class
 - 1903 ▪ whether the function needs network connectivity
- 1904 • prioritization policy for the time sensitive functions of the SHGPVA in case of CPU, memory or power
1905 resource conflict

1906 The following test setups shall be prepared:

- 1907 • the SHGPVA is set up in default configuration
- 1908 • a test setup to:
 - 1909 - read or deduced the status of the time sensitive functions from the SHGPVA
 - 1910 - induce a DOS status on the SHGPVA causing increasing demand on processing resources

1911 **Assessment activities:**

1912 The following activities shall be performed:

- 1913 • verify the correctness and completeness of the documentation
- 1914 • conceptually verify the prioritization policy
- 1915 • progressively higher the intensity of requests to induce a DOS status on the SHGPVA
 - 1916 - record the status of every time sensitive function

1917 **Assignment of verdict:**

1918 The verdict PASS shall be assigned if:

- 1919 • no indication, that the documentation is incorrect or incomplete, are found; and
- 1920 • the prioritization policy is conceptually valid; and
- 1921 • every time sensitive function:
 - 1922 - the status of the function is in accordance with the prioritization policy during DOS.

1923 The verdict FAIL shall be assigned otherwise.

1924 **Supporting Evidence:**

- 1925 • descriptions of the performed tests and records of performed tests

1926 **6.1.8.8 Assessment criteria for [AVAI-TIME-IMP-AMP]**

1927 **Assessment objective:**

1928 The assessment covers:

- 1929 • a conceptual assessment of [AVAI-TIME-NET-PRIO]
- 1930 • a functional sufficiency assessment of the SHGPVAs network amplification, to fulfil
- 1931 [AVAI-TIME-NET-PRIO]

1932 based on the default configuration required by clause [5.1.2](#).

1933 **Assessment preparation:**

1934 The following documentation for the SHGPVA shall be complete:

- 1935 • a list of all function, whose use can impact the availability of other devices, services or networks of the
- 1936 SHGPVA:
 - 1937 - for each of these functions:
 - 1938 ▪ the function, whose use can impact the availability of other devices, services or networks impact
 - 1939 class
 - 1940 ▪ a list of all used interfaces

1941 The following test setups shall be prepared:

- 1942 • the SHGPVA is set up in default configuration
- 1943 • a test setup to:
 - 1944 - execute amplification attacks against the SHGPVA
 - 1945 - measure the affective amplification of network traffic caused by the SHGPVA

1946 **Assessment activities:**

1947 The following activities shall be performed:

- 1948 • verify the correctness and completeness of the documentation
- 1949 • for every function, whose use can impact the availability of other devices, services or networks with
- 1950 IMP.FH.DSN.Medium or higher:
 - 1951 - progressively increase the intensity of an amplification attack against this function
 - 1952 - measure the affective amplification of network traffic

1953 **Assignment of verdict:**

1954 The verdict PASS shall be assigned if:

- 1955 • no indication, that the documentation is incorrect or incomplete, are found; and
- 1956 • for every function, whose use can impact the availability of other devices, services or networks with
- 1957 IMP.FH.DSN.Medium or higher:
 - 1958 - the affective amplification of network traffic is not higher than 10

1959 The verdict FAIL shall be assigned otherwise.

1960 **Supporting Evidence:**

- 1961 • descriptions of the performed tests and records of performed tests

1962 **6.1.8.9 Assessment criteria for [AVAI-TIME-DOS-RATE]**

1963 **Assessment objective:**

1964 The assessment covers:

- 1965 • a conceptual assessment of [AVAI-TIME-DOS-RATE]
- 1966 • a functional sufficiency assessment of the SHGPVAs network rate limiting, to fulfil
- 1967 [AVAI-TIME-DOS-RATE]

1968 based on the default configuration required by clause [5.1.2](#).

1969 **Assessment preparation:**

1970 The following documentation for the SHGPVA shall be complete:

- 1971 • a list of all time sensitive function of the SHGPVA:
 - 1972 - for each of these functions:
 - 1973 ▪ the time sensitive availability impact class
 - 1974 ▪ a list of all used interfaces
- 1975 • a list of all machine interface provided by the SHGPVA
- 1976 • rate limiting policy for the SHGPVA

1977 The following test setups shall be prepared:

- 1978 • the SHGPVA is set up in default configuration
- 1979 • a test setup to:
 - 1980 - induce a DOS status on the SHGPVA causing increasing demand on processing resources
 - 1981 - check the status of all time sensitive function with IMP.AVAI.TIME.High

1982 **Assessment activities:**

1983 The following activities shall be performed:

- 1984 • verify the correctness and completeness of the documentation
- 1985 • progressively higher the intensity of requests to induce a DOS status on the SHGPVA
 - 1986 - record the status of every time sensitive function with IMP.AVAI.TIME.High

1987 **Assignment of verdict:**

1988 The verdict PASS shall be assigned if:

- 1989 • no indication, that the documentation is incorrect or incomplete, are found; and
- 1990 • the rate limiting policy is conceptually valid; and
- 1991 • for every time sensitive function with IMP.AVAI.TIME.High or higher:
 - 1992 - the status of the function is in accordance with the rate limiting policy during DOS.

1993 The verdict FAIL shall be assigned otherwise.

1994 **Supporting Evidence:**

- 1995 • descriptions of the performed tests and records of performed tests

1996 **6.1.8.10 Assessment criteria for [AVAI-SUM-SCHEDULE]**

1997 **Assessment objective:**

1998 The assessment covers:

- 1999
- a conceptual assessment of [AVAI-SUM-SCHEDULE]
- 2000
- a functional sufficiency assessment of the SHGPVAs notification in case of non-availability induced by DOS,
- 2001 to fulfil [AVAI-TIME-PREV-NOT]

2002 based on the default configuration required by clause [5.1.2](#).

2003 **Assessment preparation:**

2004 The following documentation for the SHGPVA shall be complete:

- 2005
- a list of all time sensitive functions of the SHGPVA:
 - 2006 - for each of these functions:
 - 2007 ▪ the time sensitive availability impact class
 - 2008 • a list of all software update mechanisms of the SHGPVA:
 - 2009 - for each of these mechanisms:
 - 2010 ▪ whether this mechanism can effect at least one time sensitive function with
 - 2011 IMP.AVAI.TIME.Medium or higher
 - 2012 ▪ description how the software update mechanism can be configured

2013 The following test setups shall be prepared:

- 2014
- the SHGPVA is set up in default configuration

2015 **Assessment activities:**

2016 The following activities shall be performed:

- 2017
- verify the correctness and completeness of the documentation
 - 2018 • for every software update mechanism that can effect at least one time sensitive function with
 - 2019 IMP.AVAI.TIME.Medium or higher:
 - 2020 - check whether the application of software updates can be scheduled
 - 2021 - record the results

2022 **Assignment of verdict:**

2023 The verdict PASS shall be assigned if:

- 2024
- no indication, that the documentation is incorrect or incomplete, are found; and
 - 2025 • for every software update mechanism that can effect at least one time sensitive function with
 - 2026 IMP.AVAI.TIME.Medium or higher:
 - 2027 - the application of software updates can be scheduled

2028 The verdict FAIL shall be assigned otherwise.

2029 **Supporting Evidence:**

- 2030
- descriptions of the performed tests and records of performed tests

2031 **6.1.9 Impact minimization**

2032 **6.1.10 Limit attack surface**

2033 **6.1.10.1 Assessment criteria for [LAS-SBOOT]**

2034 **Assessment objective:**

2035 The assessment covers:

- 2036 • a conceptual assessment of [LAS-SBOOT]
- 2037 • a functional sufficiency assessment of the bootloader function used by the SHGPVA to fulfil [LAS-SBOOT]

2038 based on the default configuration required by clause [5.1.2](#).

2039 **Assessment preparation:**

2040 The following documentation for the SHGPVA shall be complete:

- 2041 • SBOM of the SHGPVA's hardware architectural component including information on which software's
2042 integrity and authenticity is protected by the bootloader function
- 2043 • documentation on how the bootloader function verifies the integrity and authenticity of the hardware
2044 architectural component's software

2045 The following test setup shall be prepared:

- 2046 • a test setup for installing integrity and authenticity tampered core software, including a software package
2047 including the tampered core software; or
- 2048 • a test setup for tampering the integrity of installed core software;

2049 **Assessment activities:**

- 2050 • The SHGPVA's conformity to [LAS-SBOOT] shall be validated based on the documentation.
- 2051 • The correct implementation of the bootloader function's integrity and authenticity verification of core software
2052 shall be verified based on:
 - 2053 - tampering the integrity and authenticity of installed core software or installing integrity and authenticity
2054 tampered core software; and
 - 2055 - restarting the SHGPVA's hardware architectural component

2056 NOTE: Typical results are:

- 2057 • the bootloader function refuses to execute the tampered core software (and thus does not execute application
2058 software), and
- 2059 • either halts, resets, or boots into a secure fallback and
- 2060 • an error indication is provided (e.g. via a log, an error code, an LED pattern, etc.).

2061 **Assignment of verdict:**

2062 The verdict PASS shall be assigned if:

- 2063 • the documentation indicates the SHGPVA's conformity to [LAS-SBOOT]; and
- 2064 • the SHGPVA's hardware architectural component does not execute the modified core software.

2065 Otherwise, the verdict FAIL shall be assigned.

2066 **Supporting Evidence:**

- 2067 • records of the validation of the documentation
- 2068 • descriptions of the performed tests and documentation of associated test records that verify the correct
- 2069 implementation of the bootloader function's integrity and authenticity verification

2070 6.1.11 Logging and monitoring mechanisms

2071 6.1.11.1 Assessment criteria for [LOG-LOW]

2072 **Assessment objective:**

2073 The assessment covers:

- 2074 • a conceptual assessment of [LOG-LOW]
- 2075 • a functional sufficiency assessment of logging mechanisms used by the SHGPVA to fulfil [LOG-LOW]
- 2076 based on the default configuration required by clause [5.1.2](#).

2077 **Assessment preparation:**

2078 The following documentation for the SHGPVA shall be complete:

- 2079 • list of all logging mechanisms
- 2080 • documentation on how the logging mechanisms creates logging data
- 2081 • documentation for which events logging data are created by which logging mechanism
- 2082 • documentation on where logging data are stored

2083 The following test setups shall be prepared:

- 2084 • a test user with the necessary permissions has been set up to trigger the events
- 2085 • logging mechanism are enabled on the SHGPVA such that at least all the events in the following point are
- 2086 covered
- 2087 • a test setup for triggering the following events: - change of configuration affecting core software;
- 2088 • starts, shutdowns or other changes of operational states of core software;
- 2089 • errors of the core software;
- 2090 • capturing of audio or video data by an architectural component;
- 2091 • storage of captured audio or video data, or data derived thereof

2092 **Assessment activities:**

2093 The following activities shall be performed:

- 2094 • Verify whether the *list of all logging mechanisms* is complete
- 2095 • trigger the events listed in *Assessment preparation*
- 2096 - for each event triggered: verify that logging data is created according to the documentation

2097 **Assignment of verdict:**

2098 The verdict PASS shall be assigned if:

- 2099 • the *list of all logging mechanisms* is complete; and
- 2100 • for each event listed in *Assessment preparation* that could be triggered, logging data is created

2101 The verdict FAIL shall be assigned otherwise.

2102 **Supporting Evidence:**

- 2103 • descriptions of the performed tests and records of performed tests

2104 **6.1.11.2 Assessment criteria for [LOG-MEDIUM]**

2105 **Assessment objective:**

2106 The assessment covers:

- 2107 • a conceptual assessment of [LOG-MEDIUM]
- 2108 • a functional sufficiency assessment of logging mechanisms used by the SHGPVA to fulfil [LOG-MEDIUM]

2109 based on the default configuration required by clause [5.1.2](#).

2110 **Assessment preparation:**

2111 The following documentation for the SHGPVA shall be complete:

- 2112 • list of all logging mechanisms
- 2113 • documentation on how the logging mechanisms creates logging data
- 2114 • documentation for which events logging data are created by which logging mechanism
- 2115 • documentation on where logging data are stored

2116 The following test setups shall be prepared:

- 2117 • a test user with the necessary permissions has been set up to trigger the events
- 2118 • a test setup for triggering the following events: - unsuccessful authentication attempt;
- 2119 • change of configuration affecting core software;
- 2120 • starts, shutdowns or other changes of operational states of core software;
- 2121 • errors of the core software;
- 2122 • unsuccessful attempt of an identity to gain additional privileges;
- 2123 • unsuccessful attempt of an identity to access a data asset or function asset ;
- 2124 • capturing of audio or video data by an architectural component;
- 2125 • transmission of captured audio or video data, or data derived thereof;
- 2126 • storage of captured audio or video data, or data derived thereof

2127 **Assessment activities:**

2128 The following activities shall be performed:

- 2129 • Verify whether the *list of all logging mechanisms* is complete
- 2130 • trigger the events listed in *Assessment preparation*
- 2131 - for each event triggered: verify that logging data is created according to the documentation

2132 **Assignment of verdict:**

2133 The verdict PASS shall be assigned if:

- 2134 • the *list of all logging mechanisms* is complete; and
- 2135 • for each event listed in *Assessment preparation* that could be triggered, logging data is created
- 2136 The verdict FAIL shall be assigned otherwise.

2137 **Supporting Evidence:**

- 2138 • descriptions of the performed tests and records of performed tests

2139 **6.1.11.3 Assessment criteria for [LOG-HIGH]**

2140 **Assessment objective:**

2141 The assessment covers:

- 2142 • a conceptual assessment of [LOG-HIGH]
- 2143 • a functional sufficiency assessment of logging mechanisms used by the SHGPVA to fulfil [LOG-HIGH]
- 2144 based on the default configuration required by clause [5.1.2](#).

2145 **Assessment preparation:**

2146 The following documentation for the SHGPVA shall be complete:

- 2147 • list of all logging mechanisms
- 2148 • documentation on how the logging mechanisms creates logging data
- 2149 • documentation for which events logging data are created by which logging mechanism
- 2150 • documentation on where logging data are stored

2151 The following test setups shall be prepared:

- 2152 • a test user with the necessary permissions has been set up to trigger the events
- 2153 • a test setup for triggering the following events: - every authentication attempt;
- 2154 • change of configuration affecting core software;
- 2155 • starts, shutdowns or other changes of operational states of core software;
- 2156 • change of configuration affecting application software whom realize function, whose use can cause harm of
2157 impact class high;
- 2158 • starts, shutdowns or other changes of operational states of application software whom realize function, whose
2159 use can cause harm of impact class high;
- 2160 • errors of the core software;
- 2161 • errors of the application software whom realize function, whose use can cause harm of impact class high;
- 2162 • every attempt of an identity to gain additional privileges;
- 2163 • every attempt of an identity to access a data asset or function asset ;
- 2164 • capturing of audio or video data by an architectural component;
- 2165 • transmission of captured audio or video data, or data derived thereof;
- 2166 • storage of captured audio or video data, or data derived thereof

2167 **Assessment activities:**

2168 The following activities shall be performed:

- 2169 • Verify whether the *list of all logging mechanisms* is complete
- 2170 • trigger the events listed in *Assessment preparation*
- 2171 - for each event triggered: verify that logging data is created according to the documentation

2172 **Assignment of verdict:**

2173 The verdict PASS shall be assigned if:

- 2174 • the *list of all logging mechanisms* is complete; and
- 2175 • for each event listed in *Assessment preparation* that could be triggered, logging data is created

2176 The verdict FAIL shall be assigned otherwise.

2177 **Supporting Evidence:**

- 2178 • descriptions of the performed tests and records of performed tests

2179 6.1.11.4 Assessment criteria for [LOG-TIME]

2180 **Assessment objective:**

2181 The assessment covers:

- 2182 • a functional sufficiency assessment of logging mechanisms used by the SHGPVA to fulfil [LOG-TIME]
- 2183 based on the default configuration required by clause [5.1.2](#).

2184 **Assessment preparation:**

2185 The following documentation for the SHGPVA shall be complete:

- 2186 • documentation on how the logging mechanisms creates logging data
- 2187 • documentation for which events logging data are created by which logging mechanism
- 2188 • documentation on where logging data are stored
- 2189 • documentation on the time sources and formats used by logging mechanism

2190 The following test setups shall be prepared:

- 2191 • a test user with the necessary permissions has been set up to trigger the events
- 2192 • logging mechanism are enabled on the SHGPVA such that at least all the events in the following point are covered
- 2193
- 2194 • a test setup for triggering events as described in *Assessment preparation* in clause [6.1.11.1](#) or clause [6.1.11.2](#)

2195 **Assessment activities:**

2196 The following activities shall be performed:

- 2197 • trigger the events listed in *Assessment preparation* and note the order and approximate time
- 2198 - for each event triggered: verify that the logging data contains a timestamp
- 2199 • for all events triggered: verify that the order and relative times, in which the events where triggered, is represented by the logging data
- 2200

2201 **Assignment of verdict:**

2202 The verdict PASS shall be assigned if:

- 2203 • the *list of all logging mechanisms* is complete; and
- 2204 • for each event listed in *Assessment preparation* that could be triggered, the logging data includes a timestamp;
2205 and
- 2206 • the order and relative times, in which the events where triggered, is represented by the logging data

2207 The verdict FAIL shall be assigned otherwise.

2208 **Supporting Evidence:**

- 2209 • descriptions of the performed tests and records of performed tests

2210 **6.1.11.5 Assessment criteria for [LOG-TIME-HIGH]**

2211 **Assessment objective:**

2212 The assessment covers:

- 2213 • a conceptual assessment of [LOG-TIME-HIGH]
- 2214 • a functional sufficiency assessment of logging mechanisms used by the SHGPVA to fulfil
2215 [LOG-TIME-HIGH]

2216 based on the default configuration required by clause [5.1.2](#).

2217 **Assessment preparation:**

2218 The following documentation for the SHGPVA shall be complete:

- 2219 • documentation on how the logging mechanisms creates logging data
- 2220 • documentation for which events logging data are created by which logging mechanism
- 2221 • documentation on where logging data are stored
- 2222 • documentation on the time sources and formats used by logging mechanism

2223 The following test setups shall be prepared:

- 2224 • a test user with the necessary permissions has been set up to trigger the events
- 2225 • logging mechanism are enabled on the SHGPVA such that at least all the events in the following point are
2226 covered
- 2227 • a test setup for triggering events as described in *Assessment preparation* in clause [6.1.11.3](#)

2228 **Assessment activities:**

2229 The following activities shall be performed:

- 2230 • Verify whether the documented time sources are able to produce real time data
- 2231 • trigger the events listed in *Assessment preparation* and note the time
- 2232 - for each event triggered: verify that the logging data contains a timestamp which represents the time, the
2233 event was triggered

2234 **Assignment of verdict:**

2235 The verdict PASS shall be assigned if:

- 2236 • the *list of all logging mechanisms* is complete; and

- 2237 • for each event listed in *Assessment preparation* that could be triggered, the logging data includes a timestamp
2238 which represents the time, the event was triggered

2239 The verdict FAIL shall be assigned otherwise.

2240 **Supporting Evidence:**

- 2241 • descriptions of the performed tests and records of performed tests

2242 **6.1.11.6 Assessment criteria for [LOG-STORAGE]**

2243 **Assessment objective:**

2244 The assessment covers:

- 2245 • a functional sufficiency assessment of integrity protecting secure storage mechanisms used by the SHGPVA to
2246 fulfil [LOG-STORAGE]

2247 based on the default configuration required by clause [5.1.2](#).

2248 **Assessment preparation:**

2249 The following documentation for the SHGPVA shall be complete:

- 2250 • documentation on how the logging mechanisms creates logging data
- 2251 • documentation for which events logging data are created by which logging mechanism
- 2252 • documentation on where logging data are stored
- 2253 • documentation on which integrity protecting secure storage mechanism are used to store logging data

2254 The following test setups shall be prepared:

- 2255 • a test user with the necessary permissions has been set up to trigger the events
- 2256 • logging mechanism are enabled on the SHGPVA such that at least all the events in the following point are
2257 covered
- 2258 • a test setup for triggering events as described in *Assessment preparation* in clause [6.1.11.2](#) or clause [6.1.11.3](#)
- 2259 • a test setup to safely restart the SHGPVA

2260 **Assessment activities:**

2261 The following activities shall be performed:

- 2262 • trigger the events listed in *Assessment preparation*
- 2263 • restart the SHGPVA
- 2264 • verify whether all logging data of the triggered events are still present

2265 **Assignment of verdict:**

2266 The verdict PASS shall be assigned if:

- 2267 • for each event listed in *Assessment preparation* that could be triggered, the logging data is still present after
2268 the SHGPVA was restarted

2269 The verdict FAIL shall be assigned otherwise.

2270 **Supporting Evidence:**

- 2271 • descriptions of the performed tests and records of performed tests

2272 **6.1.11.7 Assessment criteria for [LOG-BACKUP]**

2273 **Assessment objective:**

2274 The assessment covers:

- 2275 • a conceptual assessment of [LOG-BACKUP]
- 2276 • a functional sufficiency assessment of data backup mechanisms used by the SHGPVA to fulfil
- 2277 [LOG-BACKUP]

2278 based on the default configuration required by clause [5.1.2](#).

2279 **Assessment preparation:**

2280 The following documentation for the SHGPVA shall be complete:

- 2281 • documentation on how the logging mechanisms creates logging data
- 2282 • documentation for which events logging data are created by which logging mechanism
- 2283 • documentation on where logging data are stored
- 2284 • documentation on which data backup mechanism are used to backup logging data
- 2285 • documentation on logging data packed up destinations

2286 The following test setups shall be prepared:

- 2287 • a test user with the necessary permissions has been set up to trigger the events
- 2288 • logging mechanism are enabled on the SHGPVA such that at least all the events in the following point are
- 2289 covered
- 2290 • a test setup for triggering events as described in *Assessment preparation* in clause [6.1.11.3](#)
- 2291 • a test setup to access all documented logging data backup destinations

2292 **Assessment activities:**

2293 The following activities shall be performed:

- 2294 • verify whether the documentation names data backup mechanisms for logging data of all events described in
- 2295 *Assessment preparation*
- 2296 • verify whether the documented destinations, where logging data are packed up to, can store these persistently
- 2297 • trigger the events listed in *Assessment preparation*
- 2298 • wait for the automatic backup cycle for the data backup mechanism used to backup logging data
- 2299 • verify whether all logging data of the triggered events are present on the backup destinations

2300 **Assignment of verdict:**

2301 The verdict PASS shall be assigned if:

- 2302 • all logging data of events described in *Assessment preparation* have at least one data backup mechanism
- 2303 documented; and
- 2304 • all documented destinations, where logging data are packed up to, can store these persistently; and
- 2305 • all logging data of the triggered events are present on the backup destinations

2306 The verdict FAIL shall be assigned otherwise.

2307 **Supporting Evidence:**

- 2308 • descriptions of the performed tests and records of performed tests

2309 **6.1.12 Deletion mechanisms**

2310 **6.1.12.1 Assessment criteria for [DLM-PERM]**

2311 **Assessment objective:**

2312 The assessment covers:

- 2313 • a conceptual assessment of [DLM-PERM],
- 2314 • a functional completeness assessment on the SHGPVA's capabilities that are addressed by [DLM-PERM], and
- 2315 • a functional sufficiency assessment of each deletion mechanism used by the SHGPVA to fulfil [DLM-PERM]

2316 based on the default configuration required by clause [5.1.2](#).

2317 **Assessment preparation:**

2318 The following documentation for the SHGPVA shall be complete:

- 2319 • a description of each deletion mechanism, including
- 2320 - deletion scope (i.e. describing what can be deleted by this mechanism),
- 2321 - method of deletion (e.g. overwriting, access control, changing pointer address, ...),
- 2322 - method of user interaction and initiation steps,
- 2323 - whether confirmation is provided after deletion is performed,
- 2324 - multi-user handling (describing the user rights to delete other users' data)

2325 The following test setups shall be prepared:

- 2326 • a test setup that allows to identify deletion mechanisms on a sample SHGPVA in default configuration;
- 2327 • for each deletion mechanism, a test setup that allows to:
- 2328 - create representative user-related data and install applications,
- 2329 - access the storage location where data and applications are stored, and
- 2330 - see the user interaction steps (e.g. menu, dialog, confirmation after deletion)

2331 **Assessment activities:**

2332 The following activities shall be performed:

- 2333 • The SHGPVA's conformity to [DLM-PERM] shall be validated based on the documentation.
- 2334 • The correctness and completeness of the documentation shall be verified by checking that all documented
- 2335 deletion mechanisms are implemented.
- 2336 - For each deletion mechanism, its correct implementation shall be verified by:
- 2337 - generating user-related data and installing an application as a user,
- 2338 - deleting the generated user-related data and the application and
- 2339 - checking whether the

- 2340 ▪ user-related data and the application are permanently removed, e.g. by at least checking the storage
- 2341 location of the user-related data and application before and after deletion,
- 2342 ▪ deletion mechanism is easy to use with limited technical knowledge,
- 2343 ▪ user can only delete its own data in multi-user systems, and
- 2344 ▪ user is provided with clear confirmation of deletion after user-related data or a user-installed
- 2345 application have been deleted.
- 2346 • Over all deletion mechanisms, it is to be checked whether all generated sample user-related data and installed
- 2347 applications can be permanently removed.

2348 **Assignment of verdict:**

2349 The verdict PASS shall be assigned if:

- 2350 • the documentation indicates the SHGPVA's conformity with [DLM-PERM], and
- 2351 • the verification of the correctness and completeness of the documentation was successful, and
- 2352 • the verification of the correct implementation of each deletion mechanism was successful, and
- 2353 • all deletion mechanisms are able to permanently remove all generated user-related data and user-installed
- 2354 applications.

2355 The verdict FAIL shall be assigned otherwise.

2356 **Supporting Evidence:**

- 2357 • records of the validation of the documentation
- 2358 • descriptions of the performed tests and records of performed tests to verify the correctness and completeness
- 2359 of the documentation
- 2360 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each
- 2361 update mechanism and the ability of the SHGPVA to delete all generated user-related data and applications

2362 6.1.13 Other product's technical requirements specifications

2363 6.1.13.1 Assessment criteria for [USERNOT-SECREL]

2364 **Assessment objective:**

2365 The assessment covers:

- 2366 • a conceptual assessment of [USERNOT-SECREL];
- 2367 • a functional sufficiency assessment concerning [USERNOT-SECREL] for each user notification mechanism.

2368 **Assessment preparation:**

2369 The following documentation for the SHGPVA shall be complete:

- 2370 • a list of all used user notification mechanisms that can provide security-related notifications; and
- 2371 • for each used user notification mechanism that can provide security-related notifications, a description on:
 - 2372 - how it ensures that it uses a language that can be easily understood by users; and
 - 2373 - how it distinguishes the representation of security-related notifications from other notifications.

2374 The following test setups shall be prepared:

2375 • for each of the SHGPVA's used user notification mechanism that can provide security-related notifications a
2376 test setup for:

2377 - generating security-related notifications; and

2378 - (where other notifications are possible) generating other notifications.

2379 **Assessment activities:**

2380 The SHGPVA's conformity to [USERNOT-SECREL] shall be validated based on the documentation. The correctness
2381 of the implementation shall be verified by inspecting for each used user notification mechanism for security-related
2382 notifications whether:

2383 • one security-related notification is clear, understandable, intelligible, legible and can be easily understood by
2384 users; and

2385 • (where other notifications are possible), the representation of security-related notifications is clearly
2386 distinguished from other notifications.

2387 **Assignment of verdict:**

2388 The verdict PASS shall be assigned if:

2389 • the documentation indicates the SHGPVA's conformity to [USERNOT-SECREL]; and

2390 • the verification of the correct implementation of each used user notification mechanism for security-related
2391 notifications was successful.

2392 The verdict FAIL shall be assigned otherwise.

2393 **Supporting Evidence:**

2394 • records of the validation of the documentation

2395 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each
2396 used user notification mechanism for security-related notifications

2397 **6.1.13.2 Assessment criteria for [GUI-SECCONF]**

2398 **Assessment objective:**

2399 The assessment covers:

2400 • a conceptual assessment of [GUI-SECCONF];

2401 • a functional sufficiency assessment concerning [GUI-SECCONF] for each SHGPVA's GUI for
2402 security-related configuration functionality.

2403 **Assessment preparation:**

2404 The following documentation for the SHGPVA shall be complete:

2405 • a list of GUIs for security-related configuration functionality; and

2406 • for each GUI for security-related configuration functionality, a description on:

2407 - how it distinguishes the visual representation of security-related configuration options from other
2408 configuration options; and

2409 - how it ensures that it uses a language for communicating the security-related consequences of changing a
2410 security-related configuration option that can be easily understood by users; and

2411 - how it clearly highlights visually when changes to security-related configuration are made by a user.

2412 The following test setups shall be prepared:

- 2413
- a test setup for accessing each SHGPVA's GUI for security-related configuration functionality.

2414 **Assessment activities:**

2415 The SHGPVA's conformity to [GUI-SECCONF] shall be validated based on the documentation. The correctness of the
2416 implementation shall be verified by inspecting for each SHGPVA's GUI for security-related configuration functionality
2417 whether:

- 2418
- the visual representation of security-related configuration options is clearly visual distinguished from other
2419 configuration options; and
 - the consequences of one security-related configuration option is communicated in a clear, understandable,
2420 intelligible, legible manner and can be easily understood by users; and
 - the change of one security-related configuration is clearly highlighted visually.
- 2422

2423 **Assignment of verdict:**

2424 The verdict PASS shall be assigned if:

- 2425
- the documentation indicates the SHGPVA's conformity to [GUI-SECCONF]; and
 - the verification of the correct implementation of each GUI for security-related configuration functionality was
2426 successful.
2427

2428 The verdict FAIL shall be assigned otherwise.

2429 **Supporting Evidence:**

- 2430
- records of the validation of the documentation
 - descriptions of the performed tests and records of performed tests to verify the correct implementation of each
2431 GUI for security-related configuration functionality
2432

2433 **6.2 Assessment criteria for vulnerability handling activities**
2434 **related to the product**

2435 The assessment criteria specified in CEN/CLC JT013090:2026 (CEN/CLC prEN 40000-1-3) [1] shall be met for the
2436 SHGPVA based on the corresponding specified input and output.

2437

2438 Annex A (informative): Relationship between the present
2439 document and the requirements of EU Regulation
2440 2024/2847

2441 **DRAFT ANNEX A - DO NOT CONSIDER THE CONTENT - See identified gaps in Annex F**

2442 The present document has been prepared under the Commission's Standardisation request M/606 - C(2025)618 [i.3] to
2443 provide one voluntary means of conforming to the requirements of Regulation (EU) No 2024/2847 of the European
2444 Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital
2445 elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber
2446 Resilience Act).

2447 Once the present document is cited in the Official Journal of the European Union under that Regulation, compliance
2448 with the normative clauses of the present document given in table 'A.1' confers, within the limits of the scope of the
2449 present document, a presumption of conformity with the corresponding requirements of that Regulation and associated
2450 EFTA regulations.

2451
2452

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

Harmonised Standard ETSI EN 304 631					
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 [CONF-MON-HW] 5.1.5.3 [CONF-MON-UI] 5.1.5.4 [CONF-MON-API] 5.1.5.5 [CONF-CAPT-MUTE] 5.1.5.6 [CONF-CAPT-MUTE-DISABLE] 5.1.5.7 [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 [DMIN-USERINFO] 5.1.6.2 [DMIN-LOCAL] 5.1.6.3 [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 [LOG-USER-ACC] 5.1.10.8 [NKEV-MKAV] 5.1.1.1 [NKEV-SUM-SUPPORT] 5.1.1.2 [NKEV-SUM-PROVIDE] 5.1.1.3</p>	U	
---	---	----------------------	---	---	--

Harmonised Standard ETSI EN 304 631					
Requirement				Requirement Conditionality	
No	Description	Requirements of Regulation	Clause(s) of the present document	U/C	Condition
			[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 [SDC-LOG-LOW] 5.1.2.5 [USERNOT-NOSECFUC] 5.1.12.1 [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 [SDC-LOG-LOW] 5.1.2.5	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 [CONF-MON-HW] 5.1.5.3 [CONF-MON-UI] 5.1.5.4 [CONF-MON-API] 5.1.5.5 [CONF-CAPT-MUTE] 5.1.5.6 [CONF-CAPT-MUTE-DISABLE] 5.1.5.7	U	

Harmonised Standard ETSI EN 304 631					
Requirement				Requirement Conditionality	
No	Description	Requirements of Regulation	Clause(s) of the present document	U/C	Condition
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	
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 [DMIN-USERINFO] 5.1.6.2 [DMIN-LOCAL] 5.1.6.3	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	

Harmonised Standard ETSI EN 304 631					
Requirement				Requirement Conditionality	
No	Description	Requirements of Regulation	Clause(s) of the present document	U/C	Condition
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 [LOG-USER-ACC] 5.1.10.8 [NKEV-SUM-NOTIF] 5.1.1.5 [SDC-LOG-LOW] 5.1.2.5 [USERNOT-NOSECFUC] 5.1.12.1	U	
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".

2453 Presumption of conformity stays valid only as long as a reference to the present document is maintained in the list
 2454 published in the Official Journal of the European Union. Users of the present document should consult frequently the
 2455 latest list published in the Official Journal of the European Union.

2456 Other Union legislation may be applicable to the product(s) falling within the scope of the present document.

2457 Annex B (informative): Guidance for the application of the 2458 present document

2459 The following approach can be used (e.g. by manufacturers)

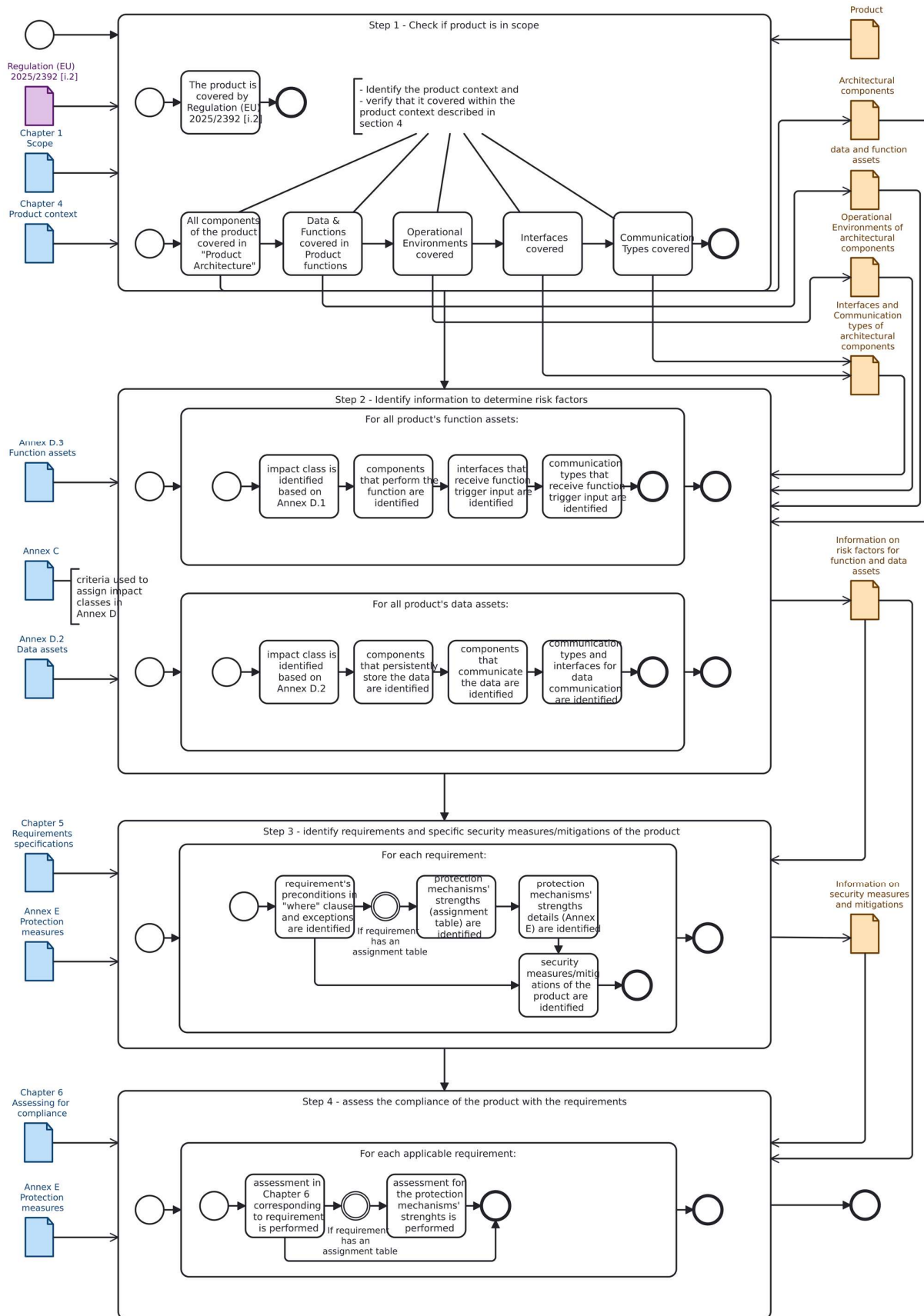
2460 • to develop products that are compliant the present document; or

2461 • to analyse the compliance of a product to the present document.

2462 The approach is constructed such that it uses parts of an assessment of cybersecurity risks and can be integrated into the
 2463 management of cybersecurity risks.

- 2464 • Step 1 - check if the product is in scope of the present document provided in clause [1](#) by:
- 2465 - verifying that the product is a SHGPVA as specified within the "technical description" of the "category
- 2466 of product" number "16." by Regulation (EU) 2025/2392 [i.2]; and
- 2467 - identifying the product context by:
- 2468 ▪ identifying the product's architectural components; and
- 2469 ▪ identifying all data processed by the product (data assets); and
- 2470 ▪ identifying all functions provided by the product (function assets); and
- 2471 ▪ identifying the architectural components' operational environments; and
- 2472 ▪ identifying the architectural components' interfaces and communication types; and
- 2473 - verifying that the product is covered within the product context described in clause [4](#) by:
- 2474 ▪ verifying that the architectural components of the product are covered within the product
- 2475 architecture described in clause [4.2](#); and
- 2476 ▪ verifying that the data processed by the product and the functions provided by the product are
- 2477 covered within clause [4.1](#); and
- 2478 ▪ verifying that the architectural components' operational environments are covered within
- 2479 clause [4.3](#); and
- 2480 ▪ verifying that the architectural components' interfaces and communication types are covered within
- 2481 clause [4.4](#).
- 2482 NOTE 1: The identification of the items mentioned above can be reused for assessing the compliance
- 2483 of the product with the requirements in clause [5](#).
- 2484 NOTE 2: If a product is a SHGPVA as specified by Regulation (EU) 2025/2392 [i.2] but is not
- 2485 covered within the product context described in clause [4](#), it is assumed that the product is not or not
- 2486 completely covered by the present document. In such cases informing ETSI Technical Committee
- 2487 Cyber Working Group for EUSR (CYBER-EUSR) via the [Committee Support Staff](#) might help to
- 2488 address those products in potential revisions of the present document.
- 2489 • Step 2 - identify information to determine risk factors by:
- 2490 - identifying for each function provided by the product:
- 2491 ▪ its impact classes according to clause [D.2](#); and
- 2492 ▪ the architectural components that perform the function; and
- 2493 ▪ the communication types and the interfaces that can receive corresponding function trigger input;
- 2494 and
- 2495 - identifying for each data processed by the product:
- 2496 ▪ its impact classes according to clause [D.1](#)
- 2497 ▪ the architectural components that persistently store the data; and
- 2498 ▪ the architectural components that can communicate the data; and
- 2499 ▪ the communication types and the interfaces over which the data is communicated.
- 2500 NOTE 3: If data processed by the product or functions provided by the product are not covered
- 2501 within clause [4.1](#), clause [C.1](#) can be used to identify impact classes for function and data assets that
- 2502 are outside the scope of the present document.

- 2503 • Step 3 - identify concrete requirements for and specific security measures/mitigations of the product that
2504 satisfy those requirements by:
- 2505 - for each requirement in clause [5](#):
- 2506 ▪ identifying the requirements applicability by evaluating the requirement's potential preconditions
2507 and exceptions based on the product's properties; and
- 2508 ▪ (for requirements that include assignment tables) identifying the required protection mechanisms'
2509 strengths (specified in annex [E](#)) by evaluating the requirement's assignment table based on the
2510 product's properties determining the attack surface and impact parameters; and
- 2511 ▪ identifying the specific security measures/mitigations that satisfy the requirement.
- 2512 NOTE 4: An assignment table can yield multiple mechanisms' strengths from different
2513 circumstances, which all have to be satisfied.
- 2514 EXAMPLE: Authentication requirements prior to changes of a SHGPVAs configuration are different
2515 whether the changes can be made via a web GUI, accessible from adjacent or public networks, a GUI,
2516 accessible from the SHGPVAs touchscreen, or a console, accessible be connecting to a serial port. All
2517 of these cases can be simultaneously present on the same SHGPVA.
- 2518 • Step 4 - assess the compliance of the product with the requirements in clause [5](#) by:
- 2519 - for each requirement in clause [5](#), performing the corresponding assessment for compliance described in
2520 clause [6](#) (the functional sufficiency assessments for different protection measures strengths are specified
2521 in annex [E](#)) by:
- 2522 ▪ preparing the assessment for the product; and
- 2523 ▪ performing the assessment activities for the product; and
- 2524 ▪ assigning an assessment verdict for the product; and
- 2525 ▪ generating the supporting evidences for the assessment.
- 2526 The figure [B.1](#) provides a graphical representation of the guidance for the application of the present document.



2528 **Figure B.1: Graphical representation on guidance for the application of the present document**

2529 **Annex C (informative): Information on the methodology for**
 2530 **the assessment of cybersecurity risks used to develop the**
 2531 **present document**

2532 **This informative annex is intended to provide information on the methodology for the assessment of**
 2533 **cybersecurity risks used to develop the present document.**

2534 C.1 Guidance for determining impact classes

2535 C.1.1 General

2536 The present document uses the following criteria to determine the impact classes of different specific SHGPVA assets
 2537 provided in annex [D](#).

2538 C.1.2 confidential data

2539 **confidentiality impact class low (IMP.CONF.Low):**

2540 The disclosure may lead to:

- 2541 • inconvenient consequences on the user(s); or
- 2542 • additional or increased attack opportunities over a short time and limited to communication types not higher
 2543 than local on the SHGPVA.

2544 **confidentiality impact class medium (IMP.CONF.Medium):**

2545 The disclosure may lead to:

- 2546 • serious impact on the user(s);
- 2547 • additional or increased attack opportunities over a short time on the SHGPVA or a limited number of other
 2548 products; or
- 2549 • additional or increased attack opportunities over a prolonged time limited to non-key-functionalities on the
 2550 SHGPVA.

2551 **confidentiality impact class high (IMP.CONF.High):**

2552 The disclosure may lead to:

- 2553 • significant or even irreversible impact on the user(s) (e.g. personal or financial harm);
- 2554 • additional or increased attack opportunities over a prolonged time on the SHGPVA or a limited number of
 2555 other products; or
- 2556 • additional or increased attack opportunities over a short time on a significant number of other products.

2557 C.1.3 loss sensitive data

2558 **loss sensitive availability impact class low (IMP.AVALLOSS.Low):**

2559 The loss may lead to:

- 2560 • inconvenient consequences on the user(s); or
- 2561 • non-availability of non-key-functionalities on the SHGPVA for a short time.

2562 **loss sensitive availability impact class medium (IMP.AVALLOSS.Medium):**

2563 The loss may lead to:

- 2564 • serious impact on the user(s); or
- 2565 • non-availability of key-functionalities of the SHGPVA over a short time; or
- 2566 • non-availability of non-key-functionalities on the SHGPVA for a prolonged time.

2567 **loss sensitive availability impact class high (IMP.AVALLOSS.High):**

2568 The loss may lead to:

- 2569 • significant or even irreversible impact on the user(s) (e.g. personal or financial harm);
- 2570 • non-availability of key-functionalities of the SHGPVA for a prolonged time; or
- 2571 • permanent non-availability of non-key-functionalities of the SHGPVA

2572 C.1.4 time sensitive data and time sensitive function

2573 **time sensitive availability impact class low (IMP.AVAL.TIME.Low):**

2574 The delay of availability may lead to:

- 2575 • non-availability of non-key-functionalities on the SHGPVA for a short time.

2576 **time sensitive availability impact class medium (IMP.AVAL.TIME.Medium):**

2577 The delay of availability may lead to:

- 2578 • non-availability of key-functionalities on the SHGPVA for a short time; or
- 2579 • non-availability of non-key-functionalities on the SHGPVA for a prolonged time.

2580 **time sensitive availability impact class high (IMP.AVAL.TIME.High):**

2581 The delay of availability may lead to:

- 2582 • non-availability of key-functionalities of the SHGPVA for a prolonged time; or
- 2583 • permanent non-availability of non-key-functionalities of the SHGPVA.

2584 C.1.5 integrity relevant data and integrity relevant function

2585 **integrity impact class low (IMP.INT.Low):**

2586 The tampering may lead to:

- 2587 • inconvenient consequences on the user(s);
- 2588 • additional or increased attack opportunities for a short time and limited to communication types not higher
2589 than local on the SHGPVA; or
- 2590 • non-availability of non-key-functionalities on the SHGPVA for a short time.

2591 **integrity impact class medium (IMP.INT.Medium):**

2592 The tampering may lead to:

- 2593 • serious impact on the user(s);
- 2594 • additional or increased attack opportunities over a short time on the SHGPVA or a limited number of other
2595 products;

2596 • additional or increased attack opportunities over a prolonged time limited to non-key-functionalities on the
2597 SHGPVA; or

2598 • non-availability of key-functionalities on the SHGPVA for a short time; or

2599 • non-availability of non-key-functionalities on the SHGPVA for a prolonged time.

2600 **integrity impact class high (IMP.INT.High):**

2601 The tampering may lead to:

2602 • significant or even irreversible impact on the user(s) (e.g. personal or financial harm);

2603 • additional or increased attack opportunities for a prolonged time on the SHGPVA or a limited number of other
2604 products;

2605 • additional or increased attack opportunities for a short time on a significant number of other products;

2606 • non-availability of key-functionalities of the SHGPVA for a prolonged time; or

2607 • permanent non-availability of non-key-functionalities of the SHGPVA

2608 Annex D (normative): Relationship between specific data
2609 and functions assets covered by the present document to
2610 impact classes for generic asset categories

2611 D.1 Data assets

2612 **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 SHGPVA data	impact class for integrity relevant SHGPVA data	impact class for time critical availability relevant SHGPVA data	impact class for loss critical availability relevant SHGPVA data
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
SHGPVA 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 SHGPVA'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)
public data asset	IMP.CONF.Low	IMP.INT.Medium	IMP.AVAI.TIME.Low	no
personal calendar data	IMP.CONF.Medium	IMP.INT.Medium	IMP.AVAI.TIME.Low	IMP.AVAI.LOSS.Medium
personal notes data	IMP.CONF.Medium	IMP.INT.Medium	IMP.AVAI.TIME.Low	IMP.AVAI.LOSS.Medium
personal contact data	IMP.CONF.Medium	IMP.INT.Medium	IMP.AVAI.TIME.Low	IMP.AVAI.LOSS.Medium
health data	IMP.CONF.High	IMP.INT.High	IMP.AVAI.TIME.Low	IMP.AVAI.LOSS.Medium
activity data	IMP.CONF.Medium	IMP.INT.Medium	IMP.AVAI.TIME.Low	IMP.AVAI.LOSS.Medium
device location data	IMP.CONF.Medium	IMP.INT.Medium	IMP.AVAI.TIME.Low	IMP.AVAI.LOSS.Low
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

2613

D.2 Function assets

2614
2615

Table D.2: Mapping of specific function assets to impact classes for generic function asset 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
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
SHGPVA function which can communicate SHGPVA 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
SHGPVA function which can modify SHGPVA 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
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

2616
2617

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

2618
2619**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
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
SHGPVA function which can communicate SHGPVA data	no	IMP.FH.DSN.Low	IMP.FH.CCON = IMP.CONF of communicated data	no
connection function	no	IMP.FH.DSN.Medium	no	no
SHGPVA function which can modify SHGPVA 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
sensing function	IMP.FH.SP = Maximum IMP.CONF of measured data	no	no	IMP.FH.MINT = Maximum IMP.INT of measured 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

2620 **Annex E (normative): Protection measures**2621 **E.1 authentication mechanism strength**2622 **E.1.1 [AUM-FH] Authentication for functions whose use can cause harm**2623 **E.1.1.1 General**

2624 The present document specifies the strength of authentication mechanisms by their resistance against certain attack
2625 types. Those attack types are constructed such that mechanisms of higher strength protect against all attack types
2626 required for lower strengths.

2627 **E.1.1.2 authentication - strength level basic**

2628 The authentication - strength level basic shall protect against the following attack types:

2629 **limited presentation attack:** Opportunistic presentation attacks on authentication mechanisms based on authentication
2630 factors of the type inheritance, using authentication factors of another entity

2631 **limited brute force attack:** Opportunistic guessing attacks on authentication mechanisms based on authentication
2632 factors of the type knowledge, by guessing manually without the use of technical aids.

2633 **E.1.1.3 authentication - strength level normal**

2634 The authentication - strength level normal shall protect against the following attack types:

2635 **automated brute force attack:** Brute force attacks on authentication mechanisms based on authentication factors of the
2636 type knowledge, by systematic try out with technical.

2637 **presentation attack:** Presentation attacks on authentication mechanisms based on authentication factors of the type
 2638 inherence, using medium effort methods like e.g. photos, cut out masks, audio replays, video replays, AI generated
 2639 voices

2640 **automated security token spoofing attack:** Security token spoofing attacks on authentication mechanisms based on
 2641 authentication factors of the type possession, by using authentication factors sourced from other uses or self-created,
 2642 without using any specific knowledge of the targeted authentication mechanisms.

2643 **replay attack:** An attacker intercepts valid data transmissions and retransmits them to mimic the original
 2644 communication partner for accepting an authentication based on the authentication factors of the type knowledge or
 2645 possession (e.g. a session token).

2646 **person in the middle attack:** An attacker secretly intercepts and alters the authentication between two parties who
 2647 believe they are communicating directly with each other based on the authentication factors of the type knowledge or
 2648 possession (e.g. a session token).

2649 E.1.1.4 authentication - strength level enhanced

2650 The authentication - strength level enhanced shall protect against the following attack types:

2651 **targeted presentation attack:** Presentation attacks on authentication mechanisms based on authentication factors of the
 2652 type inherence, using enhanced effort methods like e.g. (partial) silicone masks, layered prints

2653 **targeted brute force attack:** Brute force attacks on authentication mechanisms based on authentication factors of the
 2654 type knowledge, by systematic try out with technical aids, making use of target specific information.

2655 **targeted security token spoofing attack:** Security token spoofing attacks on authentication mechanisms based on
 2656 authentication factors of the type possession, by using authentication factors sourced from devices of the same type as
 2657 the SHGPVA or self-created, using specific knowledge of the targeted authentication mechanisms and the SHGPVA.

2658 **replay attack:** An attacker intercepts valid data transmissions and retransmits them to mimic the original
 2659 communication partner for accepting an authentication based on the authentication factors of the type knowledge or
 2660 possession (e.g. a session token).

2661 **person in the middle attack:** An attacker secretly intercepts and alters the authentication between two parties who
 2662 believe they are communicating directly with each other based on the authentication factors of the type knowledge or
 2663 possession (e.g. a session token).

2664 E.1.1.5 authentication - strength level strong

2665 The authentication - strength level strong shall protect against the following attack types:

2666 **elaborate presentation attack:** Presentation attacks on authentication mechanisms based on authentication factors of
 2667 the type inherence", using high effort methods like e.g. highly realistic silicone or latex masks, limb replicas, trained
 2668 deepfakes

2669 **elaborate brute force attack:** Brute force attacks on authentication mechanisms based on authentication factors of the
 2670 type knowledge, by systematic try out with technical aids, making use of target specific information, and unrestricted
 2671 duration.

2672 **elaborate security token spoofing attack:** Security token spoofing attacks on authentication mechanisms based on
 2673 authentication factors of the type possession, by using authentication factors created or sourced from devices of the
 2674 same type as the SHGPVA and modified, specifically for the targeted authentication mechanisms.

2675 **replay attack:** An attacker intercepts valid data transmissions and retransmits them to mimic the original
 2676 communication partner for accepting an authentication based on the authentication factors of the type knowledge or
 2677 possession (e.g. a session token).

2678 **person in the middle attack:** An attacker secretly intercepts and alters the authentication between two parties who
 2679 believe they are communicating directly with each other based on the authentication factors of the type knowledge or
 2680 possession (e.g. a session token).

2681 E.1.2 Assessment for authentication mechanism strength

2682 E.1.2.1 Assessment criteria regarding the protection against limited presentation 2683 attacks

2684 **Assessment objective:**

2685 The assessment covers functional testing of authentication mechanisms that provide a basic level of protection and use
2686 authentication factors of the type inherence against limited presentation attacks.

2687 **Assessment preparation:**

- 2688 • the SHGPVA shall be set up in default configuration
- 2689 • a genuine enrolled biometric template in the corresponding authentication mechanism with credential for
2690 authentication shall be created
- 2691 • at least one interface, where the authentication mechanism is reachable shall be documented

2692 **Assessment activities:**

- 2693 • authentication at the created genuine enrolled biometric template shall be attempted using the correct genuine
2694 enrolled biometric template identifier, if present, and authentication factors, not belonging to the person who
2695 set up the account, for at least five times or ten minutes at highest archivable query frequency
- 2696 • the outcome and used authentication factor of each attempt shall be recorded

2697 **Assignment of verdict:**

2698 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts.

2699 The verdict FAIL shall be assigned otherwise.

2700 **Supporting Evidence:**

- 2701 • description of the performed test
- 2702 • all test records of the performed test

2703 E.1.2.2 Assessment criteria regarding the protection against targeted presentation 2704 attacks

2705 **Assessment objective:**

2706 The assessment covers functional testing of authentication mechanisms that provide a enhanced level of protection and
2707 use authentication factors of the type inherence against targeted presentation attacks.

2708 **Assessment preparation:**

- 2709 • the SHGPVA shall be set up in default configuration
- 2710 • a genuine enrolled biometric template in the corresponding authentication mechanism with credential for
2711 authentication shall be created
- 2712 • at least one interface, where the authentication mechanism is reachable shall be documented
- 2713 • authentication factors shall be fabricated using common materials and tools as well as readily available source
2714 materials. The fabrication process shall not be longer than *one workday* per authentication factor.

2715 **Assessment activities:**

- 2716 • authentication at the created genuine enrolled biometric template shall be attempted using the correct genuine
2717 enrolled biometric template identifier, if present, and at least two fabricated authentication factors tried at least
2718 five times with slightly different parameters each

- 2719 • the outcome and used authentication factor of each attempt shall be recorded

2720 **Assignment of verdict:**

2721 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts.

2722 The verdict FAIL shall be assigned otherwise.

2723 **Supporting Evidence:**

- 2724 • description of the performed test
- 2725 • all test records of the performed test

2726 **E.1.2.3 Assessment criteria regarding the protection against elaborate presentation**
2727 **attacks**

2728 **Assessment objective:**

2729 The assessment covers functional testing of authentication mechanisms that provide a high level of protection and use
2730 authentication factors of the type inherence against elaborate presentation attacks.

2731 **Assessment preparation:**

- 2732 • the SHGPVA shall be set up in default configuration
- 2733 • a genuine enrolled biometric template in the corresponding authentication mechanism with credential for
2734 authentication shall be created
- 2735 • at least one interface, where the authentication mechanism is reachable shall be documented
- 2736 • authentication factors shall be fabricated using specialized materials and tools as well as cumbersome
2737 extracted source materials. The duration of the fabrication process per authentication factor is not restricted.

2738 **Assessment activities:**

- 2739 • authentication at the created genuine enrolled biometric template shall be attempted using the correct genuine
2740 enrolled biometric template identifier, if present, and at least two fabricated authentication factors tried at least
2741 five times with slightly different parameters each
- 2742 • the outcome and used authentication factor of each attempt shall be recorded

2743 **Assignment of verdict:**

2744 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts.

2745 The verdict FAIL shall be assigned otherwise.

2746 **Supporting Evidence:**

- 2747 • description of the performed test
- 2748 • all test records of the performed test

2749 **E.1.2.4 Assessment criteria regarding the protection against limited brute force**
2750 **attacks**

2751 **Assessment objective:**

2752 The assessment covers functional testing of authentication mechanisms that provide a basic level of protection and use
2753 authentication factors of the type knowledge against limited brute force attacks.

2754 **Assessment preparation:**

- 2755 • the SHGPVA shall be set up in default configuration

- 2756 • at least one interface, where the authentication mechanism is reachable shall be documented

2757 the security insurance time (T_{SI}) for this assessment is 10 minutes (600s)

2758 **Assessment activities:**

2759 the minimal recommended complexity of passwords accepted by the mechanism ($C_{PW,min}$) shall be determined;

2760 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

2761 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
2762 per login attempt + a one-hour waiting period after 5 failed login attempts

2763 the probability of guessing a completely random password of the minimal recommended complexity (p_{GRP}) shall be
2764 calculated by $p_{GRP} = T_{SI} * f_{LA,max} / C_{PW,min}$

- 2765 • the methods and outcome of each step shall be recorded

2766 **Assignment of verdict:**

2767 The verdict PASS shall be assigned if the calculated probability p_{GRP} is less than 10^{-2} .

2768 The verdict FAIL shall be assigned otherwise.

2769 **Supporting Evidence:**

- 2770 • the authentication mechanism and the interface via which it was accessed

- 2771 • all test records of the performed test

2772 **E.1.2.5 Assessment criteria regarding the protection against targeted brute force**
2773 **attacks**

2774 **Assessment objective:**

2775 The assessment covers functional testing of authentication mechanisms that provide an enhanced level of protection and
2776 use authentication factors of the type knowledge against targeted brute force attacks.

2777 **Assessment preparation:**

- 2778 • the SHGPVA shall be set up in default configuration
- 2779 • at least one interface, where the authentication mechanism is reachable shall be documented

2780 the security insurance time (T_{SI}) for this assessment one month ($2,6 * 10^6$ s)

2781 **Assessment activities:**

2782 the minimal recommended complexity of passwords accepted by the mechanism ($C_{PW,min}$) shall be determined; e.g.,
2783 $C_{PW,min} = (26 * 2 + 10)^8$ for minimum 8 characters of upper-case or lower-case letters or numbers

2784 the maximum sustained login attempt frequency ($f_{LA,max}$) shall be determined; e.g. $f_{LA,max} = (0,1s)^{-1}$ for 10 login
2785 attempt per second

2786 the probability of guessing a completely random password of the minimal recommended complexity (p_{GRP}) shall be
2787 calculated by $p_{GRP} = T_{SI} * f_{LA,max} / C_{PW,min}$

- 2788 • the methods and outcome of each step shall be recorded

2789 **Assignment of verdict:**

2790 The verdict PASS shall be assigned if the calculated probability p_{GRP} is less than 10^{-6} .

2791 The verdict FAIL shall be assigned otherwise.

2792 **Supporting Evidence:**

- 2793 • the authentication mechanism and the interface via which it was accessed
- 2794 • all test records of the performed test

2795 **E.1.2.6 Assessment criteria regarding the protection against automated brute force attacks**
27962797 **Assessment objective:**

2798 The assessment covers functional testing of authentication mechanisms that provide a medium level of protection and
2799 use authentication factors of the type knowledge against targeted brute force attacks.

2800 **Assessment preparation:**

- 2801 • the SHGPVA shall be set up in default configuration
- 2802 • at least one interface, where the authentication mechanism is reachable shall be documented

2803 the security insurance time (T_{SI}) for this assessment is one day (86400s)

2804 **Assessment activities:**

2805 the minimal recommended complexity of passwords accepted by the mechanism ($C_{PW,min}$) shall be determined;
2806 e.g. $C_{PW,min} = (26 * 2 + 10)^8$ for minimum 8 characters of upper-case case or lower-case letters or numbers

2807 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
2808 per login attempt + a one-hour waiting period after 5 failed login attempts

2809 the probability of guessing a completely random password of the minimal recommended complexity (p_{GRP}) shall be
2810 calculated by $p_{GRP} = T_{SI} * f_{LA,max} / C_{PW,min}$

- 2811 • the methods and outcome of each step shall be recorded

2812 **Assignment of verdict:**

2813 The verdict PASS shall be assigned if the calculated probability p_{GRP} is less than 10^{-6} .

2814 The verdict FAIL shall be assigned otherwise.

2815 **Supporting Evidence:**

- 2816 • the authentication mechanism and the interface via which it was accessed
- 2817 • all test records of the performed test

2818 **E.1.2.7 Assessment criteria regarding the protection against presentation attacks**2819 **Assessment objective:**

2820 The assessment covers functional testing of authentication mechanisms that provide a medium level of protection and
2821 use authentication factors of the type inherence against presentation attacks.

2822 **Assessment preparation:**

- 2823 • the SHGPVA shall be set up in default configuration
- 2824 • a genuine enrolled biometric template in the corresponding authentication mechanism with credential for
2825 authentication shall be created
- 2826 • at least one interface, where the authentication mechanism is reachable shall be documented

- 2827 • authentication factors shall be fabricated using readily available materials and tools as well as readily available
2828 source materials. The fabrication process shall not be longer than *twenty* minutes per authentication factor.

2829 NOTE: Readily available source materials are e.g. fingerprints on everyday items or publicly available photos.
2830 Readily available materials and tools are of adhesive tape, printer paper, common printers.

2831 **Assessment activities:**

- 2832 • authentication at the created account shall be attempted using the correct account name, if present, and at least
2833 two fabricated authentication factors tried at least five times with slightly different parameters each
- 2834 • the outcome and used fabricated authentication factor of each attempt shall be recorded

2835 **Assignment of verdict:**

2836 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts.

2837 The verdict FAIL shall be assigned otherwise.

2838 **Supporting Evidence:**

- 2839 • description of the performed test
- 2840 • all test records of the performed test

2841 **E.1.2.8 Assessment criteria regarding the protection against elaborate brute force**
2842 **attacks**

2843 **Assessment objective:**

2844 The assessment covers functional testing of authentication mechanisms that provide a high level of protection and use
2845 authentication factors of the type knowledge against targeted brute force attacks.

2846 **Assessment preparation:**

- 2847 • the SHGPVA shall be set up in default configuration
- 2848 • at least one interface, where the authentication mechanism is reachable shall be documented

2849 the security insurance time (T_{SI}) for this assessment is five years ($1,6 * 10^8 s$)

2850 **Assessment activities:**

- 2851 the minimal recommended complexity of passwords accepted by the mechanism ($C_{PW,min}$) shall be determined;
2852 e.g. $(26 * 2 + 10)^8$ for minimum 8 characters of upper-case case or lower-case letters or numbers
- 2853 the maximum sustained login attempt frequency ($f_{LA,max}$) shall be determined; e.g. $(0,1s)^{-1}$ for 10 login attempt per
2854 second
- 2855 the probability of guessing a completely random password of the minimal recommended complexity (p_{GRP}) shall be
2856 calculated by $p_{GRP} = T_{SI} * f_{LA,max} / C_{PW,min}$
- 2857 • the methods and outcome of each step shall be recorded

2858 **Assignment of verdict:**

2859 The verdict PASS shall be assigned if the calculated probability is less than 10^{-6} .

2860 The verdict FAIL shall be assigned otherwise.

2861 **Supporting Evidence:**

- 2862 • the authentication mechanism and the interface via which it was accessed
- 2863 • all test records of the performed test

2864 E.1.2.9 Assessment criteria regarding the protection against automated security
2865 token spoofing attacks

2866 **Assessment objective:**

2867 The assessment covers functional testing of authentication mechanisms that provide a medium level of protection and
2868 use authentication factors of the type possession against automated security token spoofing attacks.

2869 **Assessment preparation:**

- 2870 • the SHGPVA shall be set up in default configuration
- 2871 • an account in the corresponding authentication mechanism with a security token for authentication shall be
2872 created
- 2873 • at least one interface, where the authentication mechanism is reachable shall be documented
- 2874 • security tokens, that match specifications of the interfaces, via which the authentication mechanism is
2875 reachable, shall be prepared or created without using any specific knowledge of the authentication mechanism

2876 **Assessment activities:**

- 2877 • authentication at the created account shall be attempted using the correct account name, if present, and the
2878 prepared or created security tokens
- 2879 • the outcome and used authentication factor of each attempt shall be recorded

2880 **Assignment of verdict:**

2881 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts, except where the used
2882 authentication factor exactly matches the configured one.

2883 The verdict FAIL shall be assigned otherwise.

2884 **Supporting Evidence:**

- 2885 • description of the performed test
- 2886 • all test records of the performed test

2887 E.1.2.10 Assessment criteria regarding the protection against targeted security token
2888 spoofing attacks

2889 **Assessment objective:**

2890 The assessment covers functional testing of authentication mechanisms that provide an enhanced level of protection and
2891 use authentication factors of the type possession against targeted security token spoofing attacks.

2892 **Assessment preparation:**

- 2893 • the SHGPVA shall be set up in default configuration
- 2894 • an account in the corresponding authentication mechanism with a security token for authentication shall be
2895 created
- 2896 • at least one interface, where the authentication mechanism is reachable shall be documented
- 2897 • security tokens, shall be prepared or created, which match the specifications of the authentication mechanism.

2898 **Assessment activities:**

- 2899 • authentication at the created account shall be attempted using the correct account name, if present, and the
2900 prepared or created security tokens
- 2901 • the outcome and used authentication factor of each attempt shall be recorded

2902 **Assignment of verdict:**

2903 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts, except where the used
2904 authentication factor exactly matches the configured one.

2905 The verdict FAIL shall be assigned otherwise.

2906 **Supporting Evidence:**

- 2907 • description of the performed test
- 2908 • all test records of the performed test

2909 **E.1.2.11 Assessment criteria regarding the protection against elaborate security token**
2910 **spoofing attacks**

2911 **Assessment objective:**

2912 The assessment covers functional testing of authentication mechanisms that provide a high level of protection and use
2913 authentication factors of the type possession against elaborate security token spoofing attacks.

2914 **Assessment preparation:**

- 2915 • the SHGPVA shall be set up in default configuration
- 2916 • an account in the corresponding authentication mechanism with a security token for authentication shall be
2917 created
- 2918 • at least one interface, where the authentication mechanism is reachable shall be documented
- 2919 • security tokens, shall be prepared or created, which match the specifications of the authentication mechanism
2920 and use information extracted from the original security token.

2921 **Assessment activities:**

- 2922 • authentication at the created account shall be attempted using the correct account name, if present, and the
2923 prepared or created security tokens
- 2924 • the outcome and used authentication factor of each attempt shall be recorded

2925 **Assignment of verdict:**

2926 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts, except where the used
2927 authentication factor exactly matches the configured one.

2928 The verdict FAIL shall be assigned otherwise.

2929 **Supporting Evidence:**

- 2930 • description of the performed test
- 2931 • all test records of the performed test

2932 **E.1.2.12 Assessment criteria regarding the protection against replay attacks**

2933 **Assessment objective:**

2934 The assessment covers functional testing of authentication mechanisms that use authentication factors of the type
2935 knowledge or possession (e.g. a session token) against replay attacks.

2936 **Assessment preparation:**

- 2937 • the SHGPVA shall be set up in default configuration
- 2938 • the authentication mechanism shall be active

- 2939 • a communication partner with active authentication mechanisms shall be set up for the SHGPVA
- 2940 • a capture and replay tool between SHGPVA and its communication partner shall be set up
- 2941 • at least one interface, where the authentication mechanism is reachable shall be documented

2942 **Assessment activities:**

- 2943 • Initiate a connection between the SHGPVA and its communication partner.
- 2944 • Use a capture tool to record the transmitted message or transaction data.
- 2945 • Replay (retransmit) the captured message to the product using a suitable tool in place to mimic the original
2946 communication partner.
- 2947 • Record if the product accepts the retransmitted data

2948 **Assignment of verdict:**

2949 The verdict PASS shall be assigned if it is not possible to impersonate as the communication partner.

2950 The verdict FAIL shall be assigned otherwise.

2951 **Supporting Evidence:**

- 2952 • description of the performed test
- 2953 • all test records of the performed test

2954 **E.1.2.13 Assessment criteria regarding the protection against PitM attacks**

2955 **Assessment objective:**

2956 The assessment covers functional testing of authentication mechanisms that use authentication factors of the type
2957 knowledge or possession (e.g. a session token) against PitM attacks.

2958 **Assessment preparation:**

- 2959 • the SHGPVA shall be set up in default configuration
- 2960 • the authentication mechanism shall be active
- 2961 • a communication partner with active authentication mechanisms shall be set up for the SHGPVA
- 2962 • a capture and PitM tool between SHGPVA and its communication partner shall be set up
- 2963 • at least one interface, where the authentication mechanism is reachable shall be documented

2964 **Assessment activities:**

- 2965 • Initiate a connection between the SHGPVA and its communication partner.
- 2966 • Attempt to capture data (user credentials, tokens, etc.) with the tool in place and actively intercept
2967 communication to impersonate the communication partner during:
 - 2968 - generation and communication of authentication factors for the communication partner (if not
2969 pre-configured); and
 - 2970 - authentication of the communication partner
- 2971 • Record if the impersonation as communication partner is successful

2972 **Assignment of verdict:**

2973 The verdict PASS shall be assigned if it is not possible to impersonate as the communication partner.

2974 The verdict FAIL shall be assigned otherwise.

2975 **Supporting Evidence:**

- 2976 • description of the performed test
- 2977 • all test records of the performed test

2978 **E.2 integrity protection strength**

2979 **E.2.1 [INT-SWPCK] Software package verification**

2980 **E.2.1.1 General**

2981 The present document specifies software package verification mechanisms' strength, by certain protection measures.
2982 Those measures are constructed such that measures of higher strength typically have less attack vectors than lower
2983 strength measures.

2984 **E.2.1.2 software package integrity verification - strength level basic**

2985 Mechanisms for the software package integrity verification - strength level basic shall:

- 2986 • explicitly obtain the confirmation of an authorized entity that the integrity and authenticity of a software
2987 package has been verified by the entity, where the software package's source is determined by the entity; or
- 2988 • explicitly obtain the confirmation of an authorized entity that the authenticity of a software package has been
2989 verified by the entity and use a hash or checksum provided by the entity for the software package to verify its
2990 integrity, where the software package's source is determined by the entity.

2991 **E.2.1.3 software package integrity verification - strength level normal**

2992 Mechanisms for the software package integrity verification - strength level normal shall ensure that a software package
2993 has been obtained from a trusted source over a secure communication channel that meets INT.COM.Enhanced.

2994 **E.2.1.4 software package integrity verification - strength level enhanced**

2995 Mechanisms for the software package integrity verification - strength level enhanced shall verify the authenticity and
2996 integrity of a software package using cryptographic digital signature verification.

2997 **E.2.2 [INT-COM] Communication of integrity relevant data**

2998 **E.2.2.1 General**

2999 The present document specifies the strength of mechanisms to protect the integrity of communicated integrity relevant
3000 data by their resistance against certain attack types. Those attack types are constructed such that mechanisms of higher
3001 strength protect against all attack types required for lower strengths.

3002 **E.2.2.2 communication of integrity relevant data - protection strength level basic**

3003 The communication of integrity relevant data - protection strength level basic shall protect against the following attack
3004 types:

3005 **accidental bit flip:** Accidental change of data by natural causes.

3006 **E.2.2.3 communication of integrity relevant data - protection strength level normal**

3007 The communication of integrity relevant data - protection strength level normal shall protect against the following
3008 attack types:

3009 **replay attack:** An attacker intercepts valid transmissions and then retransmits those captured messages to the same
3010 interface to deceive it into performing unauthorized actions.

3011 **accidental bit flip:** Accidental change of data by natural causes.

- 3012 **direct identity spoofing attack:** An attacker mimics another entity to gain a trust relationship with the SHGPVA
- 3013 **downgrade of communication protocols attack:** An attacker forces to use of a legacy, less secure, communication
3014 protocol
- 3015 **E.2.2.4 communication of integrity relevant data - protection strength level enhanced**
- 3016 The communication of integrity relevant data - protection strength level enhanced shall protect against the following
3017 attack types:
- 3018 **replay attack:** An attacker intercepts valid transmissions and then retransmits those captured messages to the same
3019 interface to deceive it into performing unauthorized actions.
- 3020 **person in the middle attack:** An attacker secretly alters the communication between the SHGPVA and another entity
3021 or another part of the SHGPVA to gain a trusted relationship with the involved communication partners without their
3022 knowledge.
- 3023 **accidental bit flip:** Accidental change of data by natural causes.
- 3024 **direct identity spoofing attack:** An attacker mimics another entity to gain a trust relationship with the SHGPVA
- 3025 **downgrade of communication protocols attack:** An attacker forces to use of a legacy, less secure, communication
3026 protocol
- 3027 **E.2.2.5 communication of integrity relevant data - protection strength level strong**
- 3028 The communication of integrity relevant data - protection strength level strong shall protect against the following attack
3029 types:
- 3030 **replay attack:** An attacker intercepts valid transmissions and then retransmits those captured messages to the same
3031 interface to deceive it into performing unauthorized actions.
- 3032 **person in the middle attack:** An attacker secretly alters the communication between the SHGPVA and another entity
3033 or another part of the SHGPVA to gain a trusted relationship with the involved communication partners without their
3034 knowledge.
- 3035 **accidental bit flip:** Accidental change of data by natural causes.
- 3036 **direct identity spoofing attack:** An attacker mimics another entity to gain a trust relationship with the SHGPVA
- 3037 **downgrade of communication protocols attack:** An attacker forces to use of a legacy, less secure, communication
3038 protocol
- 3039 **E.3 confidentiality protection strength**
- 3040 **E.3.1 [CONF-SSM] Confidentiality protecting persistent storage for
3041 confidential data**
- 3042 **E.3.1.1 General**
- 3043 The present document specifies confidentiality protecting secure storage mechanisms' strength, by certain security
3044 properties. Those properties are constructed such that mechanisms of higher strength have the properties of lower
3045 strength mechanisms.
- 3046 **E.3.1.2 confidential persistent storage - strength level basic**
- 3047 Mechanisms for the confidential persistent storage - strength level basic shall encrypt such that decryption is only
3048 possible for the SHGPVA.
- 3049 **E.3.1.3 confidential persistent storage - strength level normal**
- 3050 Mechanisms for the confidential persistent storage - strength level normal shall encrypt such that decryption is

3051 • only possible for the SHGPVA and

3052 • only performed after a successful authentication.

3053 E.3.1.4 confidential persistent storage - strength level enhanced

3054 Mechanisms for the confidential persistent storage - strength level enhanced shall encrypt supported by hardware, such
3055 that

3056 • decryption is only possible for the SHGPVA after a successful authentication and

3057 • the extraction of the encryption key is prevented by hardware.

3058 E.3.1.5 confidential persistent storage - strength level strong

3059 Mechanisms for the confidential persistent storage - strength level strong shall prevent the extraction of data by
3060 hardware.

3061 E.3.2 [CONF-COM] Communication of confidential data

3062 E.3.2.1 General

3063 The present document specifies the strength of mechanisms to protect the confidentiality of communicated confidential
3064 data by their resistance against certain attack types. Those attack types are constructed such that mechanisms of higher
3065 strength protect against all attack types required for lower strengths.

3066 E.3.2.2 authentication - strength level strong

3067 The authentication - strength level strong shall protect against the following attack types:

3068 **eavesdropping:** An attacker secretly intercepts the communication between the SHGPVA and another entity or another
3069 part of the SHGPVA.

3070 E.3.2.3 communication of confidential data - protection strength level normal

3071 The communication of confidential data - protection strength level normal shall protect against the following attack
3072 types:

3073 **eavesdropping:** An attacker secretly intercepts the communication between the SHGPVA and another entity or another
3074 part of the SHGPVA.

3075 **direct identity spoofing attack:** An attacker mimics another entity to gain a trust relationship with the SHGPVA

3076 **downgrade of communication protocols attack:** An attacker forces to use of a legacy, less secure, communication
3077 protocol

3078 E.3.2.4 communication of confidential data - protection strength level enhanced

3079 The communication of confidential data - protection strength level enhanced shall protect against the following attack
3080 types:

3081 **eavesdropping:** An attacker secretly intercepts the communication between the SHGPVA and another entity or another
3082 part of the SHGPVA.

3083 **person in the middle attack:** An attacker secretly alters the communication between the SHGPVA and another entity
3084 or another part of the SHGPVA to gain a trusted relationship with the involved communication partners without their
3085 knowledge.

3086 **direct identity spoofing attack:** An attacker mimics another entity to gain a trust relationship with the SHGPVA

3087 **downgrade of communication protocols attack:** An attacker forces to use of a legacy, less secure, communication
3088 protocol

3089 E.3.2.5 communication of confidential data - protection strength level strong

3090 The communication of confidential data - protection strength level strong shall protect against the following attack
3091 types:

3092 **eavesdropping**: An attacker secretly intercepts the communication between the SHGPVA and another entity or another
3093 part of the SHGPVA.

3094 **person in the middle attack**: An attacker secretly alters the communication between the SHGPVA and another entity
3095 or another part of the SHGPVA to gain a trusted relationship with the involved communication partners without their
3096 knowledge.

3097 **direct identity spoofing attack**: An attacker mimics another entity to gain a trust relationship with the SHGPVA

3098 **downgrade of communication protocols attack**: An attacker forces to use of a legacy, less secure, communication
3099 protocol

3100 **Annex F (informative): Relationship between the present**
3101 **document and the covered/not covered cybersecurity risks**

3102 **This informative annex is intended to provide the relevant information on the covered/not covered cybersecurity**
3103 **risks and still under discussion.**

3104 **The information provided in the column "Risk coverage" is based on a preliminary analysis which is planned to**
3105 **be expanded in the future and still under discussion.**

3106

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 SHGPVA		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 [LOG-USER-ACC] 5.1.10.8 [SDC-LOG-LOW] 5.1.2.5 [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 SHGPVA				N
[3]	A threat actor	tamper s	integrity relevant data	volatile stored on the SHGPVA				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 SHGPVA	unnecessarily processed	Prevention: [CONF-CAPT-MUTE] 5.1.5.6 [CONF-CAPT-MUTE-DISABLE] 5.1.5.7 [DMIN-DJST] 5.1.6.1 Information: [CONF-MON-HW] 5.1.5.3 [CONF-MON-UI] 5.1.5.4 [CONF-MON-API] 5.1.5.5 [DMIN-USERINFO] 5.1.6.2		C
[6]	A threat actor	discloses	confidential data	permanently stored on the SHGPVA	during storage	Prevention: [CONF-SSM] 5.1.5.1	POE	C
[7]	A threat actor	discloses	confidential data	permanently stored on the SHGPVA	after deletion	Prevention: [DLM-PERM] 5.1.11.1		N
[8]	A threat actor	discloses	confidential data	volatile stored on the SHGPVA	during usage			N
[9]	A threat actor	discloses	confidential data	volatile stored on the SHGPVA	after usage			N
[10]	A threat actor	discloses	confidential data	communicated from or to the architectural component		Prevention: [CONF-COM] 5.1.5.2 [DMIN-LOCAL] 5.1.6.3	COM, IF and POE	C

No.	Threat Actor	Threat action	Asset	Threat details		Requirement(s) for mitigation	Relevant attack surface parameter	Risk coverage
[11]	A threat actor	tamper s	loss sensitive data	permanently stored on the SHGPVA	during storage			N
[12]	A threat actor	tamper s	integrity relevant function	on the SHGPVA		Prevention: [INT-SWPCK] 5.1.4.1 [LAS-SBOOT] 5.1.9.6		N
[13]	A threat actor	impact s the availability of	time sensitive function	on the SHGPVA	by interruption caused by a software update installation	Prevention: [AVAI-SUM-SCHEDULE] 5.1.7.10		C
[14]	A threat actor	impact s the availability of	time sensitive function	on the SHGPVA	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	impact s the availability of	time sensitive function	on the SHGPVA	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	impact s the availability of	time sensitive function	on the SHGPVA	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	exploit s 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 an incorrect actions		on the SHGPVA		Prevention: [GUI-SECCONF] 5.1.12.3 Information: [GUI-SECCONF] 5.1.12.3	IF.Human	C

No.	Threat Actor	Threat action	Asset	Threat details		Requirement(s) for mitigation	Relevant attack surface parameter	Risk coverage
[19]	A user	performs insecure actions		on the SHGPVA	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
[20]	A user	unknowingly creates confidential	audio or video capture data	on the SHGPVA		Prevention: [CONF-CAPT-MUTE] 5.1.5.6 [CONF-CAPT-MUTE-DISABLE] 5.1.5.7 Information: [CONF-MON-HW] 5.1.5.3 [CONF-MON-UI] 5.1.5.4 [CONF-MON-API] 5.1.5.5	IF.Human	C

- 3107
- 3108
- The columns *Threat Actor*, *Threat Action*, *Asset*, and *Threat Details* describe the threat scenario under consideration.
- 3109
- 3110
- The column *Requirement(s) for mitigation* refers to the mitigations of the risks that arise from the threat scenario.
- 3111
- 3112
- The *Relevant attack surface parameter* column describes which of the attack surface parameters make a difference in mitigation.
- 3113
- 3114
- 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).

3115 **Annex G (informative): Relationship between the present**

3116 **document and ETSI EN 303 645/ ETSI TS 103 701**

3117 **This informative annex is intended to provide a mapping between the present document and the content of ETSI**

3118 **TC CYBER's existing work on CIoT devices (ETSI EN 303 645/ ETSI TS 103 701).**