



Cyber Security (CYBER); Cyber Resilience Act (CRA); Cybersecurity requirements for internet connected toys

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-004 >

Keywords

< CRA;Cybersecurity >

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.....		16
13	4 Product context.....		18
14	4.1 Product functions		18
15	4.1.1 Essential Functions.....		18
16	4.1.2 Supporting functions		18
17	4.1.3 Data assets.....		19
18	4.2 Product Architecture.....		19
19	4.3 Operational Environment.....		20
20	4.4 Interfaces.....		21
21	4.5 Distribution of security functions		21
22	4.6 Users		21
23	4.7 Use cases.....		22
24	4.7.1 General		22
25	4.7.2 Use case profiles		22
26	4.8 Security Profiles.....		22
27	5 Requirements specifications.....		23
28	5.1 Product's technical requirements specifications.....		23
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.....		24
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-PARCONT] Default configuration for parental control.....		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 [PARCONT] Support of parental control.....		26
44	5.1.3.3 [AUM-FH] Authentication for functions whose use can cause harm.....		26
45	5.1.3.4 [AUTHZ-LP] Least privilege in authorization policies.....		27
46	5.1.3.5 [AUTHZ-R] Revocability of granted permissions		27
47	5.1.3.6 [AUTHZ-PC] Authorization policies for parental control.....		27
48	5.1.4 Integrity protection.....		27
49	5.1.4.1 [INT-SWPCK] Software package verification		27
50	5.1.4.2 [INT-COM] Communication of integrity relevant data.....		27
51	5.1.5 Confidentiality protection		28
52	5.1.5.1 [CONF-SSM] Confidentiality protecting persistent storage for confidential data		28
53	5.1.5.2 [CONF-COM] Communication of confidential data.....		28

54	5.1.6	Data minimization	29
55	5.1.6.1	[DMIN-DJST] Documented justification of processed data	29
56	5.1.7	Availability protection	29
57	5.1.7.1	[AVAI-TIME-RECO-POW] Restoration after loss of power	29
58	5.1.7.2	[AVAI-TIME-NETW] Local operation	29
59	5.1.7.3	[AVAI-TIME-RECO-NETW] Restoration after loss of network connection	29
60	5.1.7.4	[AVAI-TIME-OUTA-NOT] Notify non-availability	29
61	5.1.7.5	[AVAI-TIME-PREV-NOT] Notify upcoming limitation	29
62	5.1.7.6	[AVAI-TIME-NET-PRIO] Network prioritization	29
63	5.1.7.7	[AVAI-TIME-RES-PRIO] Power resource prioritization	30
64	5.1.7.8	[AVAI-TIME-IMP-AMP] Amplification control	30
65	5.1.7.9	[AVAI-TIME-DOS-RATE] Incoming rate limiting	30
66	5.1.7.10	[AVAI-SUM-SCHEDULE] Scheduling of updates	30
67	5.1.8	Impact minimization	30
68	5.1.9	Limit attack surface	30
69	5.1.9.1	[LAS-INVAL] Validation of external data input	30
70	5.1.9.2	[LAS-INSAN] Sanitization of external data input	31
71	5.1.9.3	[LAS-PHY-INF] Only necessary physical interfaces	31
72	5.1.9.4	[LAS-LOGIC-INF] Only necessary logical interfaces active by default	31
73	5.1.9.5	[LAS-APP] Only necessary apps by default	31
74	5.1.9.6	[LAS-SBOOT] Secure boot	31
75	5.1.10	Logging and monitoring mechanisms	31
76	5.1.10.1	[LOG-LOW] Events to log for low risk internet connected toy	31
77	5.1.10.2	[LOG-MEDIUM] Events to log for medium risk internet connected toy	31
78	5.1.10.3	[LOG-HIGH] Events to log for high risk internet connected toy	32
79	5.1.10.4	[LOG-TIME] Timestamps for logs	32
80	5.1.10.5	[LOG-TIME-HIGH] Real-Timestamps for logs	32
81	5.1.10.6	[LOG-STORAGE] Persistently store logfiles	32
82	5.1.10.7	[LOG-BACKUP] Backup of logfiles	32
83	5.1.11	Deletion mechanisms	32
84	5.1.11.1	[DLM-PERM] Permanent removal of user-related data	32
85	5.1.12	Other product's technical requirements specifications	33
86	5.1.12.1	[USERNOT-NOSECFUC] User notifications on not available security functions	33
87	5.1.12.2	[USERNOT-SECREL] Language and representation for security-related user notifications	33
88	5.1.12.3	[GUI-SECONF] Visual representation of security-related configuration via GUIs	33
89	5.1.12.4	[CRY-SOTA] State-of-the-art cryptography	33
90	5.1.12.5	[CRY-CCK-PRE-LEN] Key size of preinstalled confidential cryptographic keys	33
91	5.1.12.6	[CRY-CCK-GEN] Default key size of generated confidential cryptographic keys	33
92	5.1.12.7	[CRY-PW-PRE-COM] Complexity of preinstalled passwords	34
93	5.1.12.8	[CRY-PW-GEN-COM] Default complexity of generated passwords	34
94	5.1.12.9	[CRY-PW-USR-COM] Recommended complexity of user chosen passwords	34
95	5.2	Requirements specifications for vulnerability handling activities related to the product	34
96	6	Assessing for compliance with requirements	34
97	6.1	Assessing for compliance with product's technical requirements specifications	34
98	6.1.1	General	34
99	6.1.2	Known exploitable vulnerabilities	34
100	6.1.2.1	Assessment criteria for [NKEV-SUM-SUPPORT]	34
101	6.1.2.2	Assessment criteria for [NKEV-SUM-PROVIDE]	36
102	6.1.2.3	Assessment criteria for [NKEV-SUM-AUTO]	37
103	6.1.2.4	Assessment criteria for [NKEV-SUM-NOTIF]	38
104	6.1.3	Default configuration	39
105	6.1.3.1	Assessment criteria for [SDC-AUM-FH]	39
106	6.1.3.2	Assessment criteria for [SDC-FRM]	40
107	6.1.4	Authentication and access control mechanisms	41
108	6.1.4.1	Assessment criteria for [ACM-FH]	41
109	6.1.4.2	Assessment criteria for [AUM-FH]	42
110	6.1.4.3	Assessment criteria for [AUTHZ-LP]	43
111	6.1.4.4	Assessment criteria for [AUTHZ-R]	44
112	6.1.5	Integrity protection	45
113	6.1.6	Confidentiality protection	45

114	6.1.7	Data minimization	45
115	6.1.7.1	Assessment criteria for [DMIN-DJST].....	45
116	6.1.8	Availability protection.....	45
117	6.1.8.1	Assessment criteria for [AVAI-TIME-RECO-POW].....	45
118	6.1.8.2	Assessment criteria for [AVAI-TIME-NETW].....	47
119	6.1.8.3	Assessment criteria for [AVAI-TIME-RECO-NETW].....	48
120	6.1.8.4	Assessment criteria for [AVAI-TIME-OUTA-NOT].....	50
121	6.1.8.5	Assessment criteria for [AVAI-TIME-PREV-NOT].....	51
122	6.1.8.6	Assessment criteria for [AVAI-TIME-NET-PRIO].....	53
123	6.1.8.7	Assessment criteria for [AVAI-TIME-RES-PRIO].....	54
124	6.1.8.8	Assessment criteria for [AVAI-TIME-IMP-AMP].....	55
125	6.1.8.9	Assessment criteria for [AVAI-TIME-DOS-RATE].....	56
126	6.1.8.10	Assessment criteria for [AVAI-SUM-SCHEDULE].....	57
127	6.1.9	Impact minimization	58
128	6.1.10	Limit attack surface.....	58
129	6.1.10.1	Assessment criteria for [LAS-SBOOT].....	58
130	6.1.11	Logging and monitoring mechanisms	59
131	6.1.11.1	Assessment criteria for [LOG-LOW].....	59
132	6.1.11.2	Assessment criteria for [LOG-MEDIUM].....	60
133	6.1.11.3	Assessment criteria for [LOG-HIGH].....	61
134	6.1.11.4	Assessment criteria for [LOG-TIME].....	62
135	6.1.11.5	Assessment criteria for [LOG-TIME-HIGH].....	63
136	6.1.11.6	Assessment criteria for [LOG-STORAGE].....	64
137	6.1.11.7	Assessment criteria for [LOG-BACKUP].....	65
138	6.1.12	Deletion mechanisms	66
139	6.1.12.1	Assessment criteria for [DLM-PERM].....	66
140	6.1.13	Other product's technical requirements specifications	67
141	6.1.13.1	Assessment criteria for [USERNOT-SECRET].....	67
142	6.1.13.2	Assessment criteria for [GUI-SECCONF].....	68
143	6.2	Assessment criteria for vulnerability handling activities related to the product	69
144	Annex A (informative):	Relationship between the present document and the requirements of	
145		EU Regulation 2024/2847	70
146	Annex B (informative):	Guidance for the application of the present document	76
147	Annex C (informative):	Information on the methodology for the assessment of cybersecurity	
148		risks used to develop the present document	80
149	C.1	Guidance for determining impact classes	80
150	C.1.1	General.....	80
151	C.1.2	confidential data.....	80
152	C.1.3	loss sensitive data.....	80
153	C.1.4	time sensitive data and time sensitive function	81
154	C.1.5	integrity relevant data and integrity relevant function.....	81
155	Annex D (normative):	Relationship between specific data and functions assets covered by	
156		the present document to impact classes for generic asset categories	83
157	D.1	Data assets	83
158	D.2	Function assets.....	83
159	Annex E (normative):	Protection measures.....	85
160	E.1	authentication mechanism strength.....	85
161	E.1.1	[AUM-FH] Authentication for functions whose use can cause harm	85
162	E.1.1.1	General	85
163	E.1.1.2	authentication - strength level basic	85
164	E.1.1.3	authentication - strength level normal	86
165	E.1.1.4	authentication - strength level enhanced.....	86
166	E.1.1.5	authentication - strength level strong.....	86
167	E.1.2	Assessment for authentication mechanism strength.....	87
168	E.1.2.1	Assessment criteria regarding the protection against limited presentation attacks	87
169	E.1.2.2	Assessment criteria regarding the protection against targeted presentation attacks	87

170	E.1.2.3	Assessment criteria regarding the protection against elaborate presentation attacks.....	88
171	E.1.2.4	Assessment criteria regarding the protection against limited brute force attacks.....	89
172	E.1.2.5	Assessment criteria regarding the protection against targeted brute force attacks.....	89
173	E.1.2.6	Assessment criteria regarding the protection against automated brute force attacks.....	90
174	E.1.2.7	Assessment criteria regarding the protection against presentation attacks	90
175	E.1.2.8	Assessment criteria regarding the protection against elaborate brute force attacks.....	91
176	E.1.2.9	Assessment criteria regarding the protection against automated security token spoofing attacks.....	92
177	E.1.2.10	Assessment criteria regarding the protection against targeted security token spoofing attacks.....	92
178	E.1.2.11	Assessment criteria regarding the protection against elaborate security token spoofing attacks.....	93
179	E.1.2.12	Assessment criteria regarding the protection against replay attacks.....	94
180	E.1.2.13	Assessment criteria regarding the protection against PitM attacks.....	94
181	E.2	integrity protection strength.....	95
182	E.2.1	[INT-SWPCK] Software package verification.....	95
183	E.2.1.1	General	95
184	E.2.1.2	software package integrity verification - strength level basic.....	95
185	E.2.1.3	software package integrity verification - strength level normal.....	95
186	E.2.1.4	software package integrity verification - strength level enhanced.....	95
187	E.2.2	[INT-COM] Communication of integrity relevant data	95
188	E.2.2.1	General	95
189	E.2.2.2	communication of integrity relevant data - protection strength level basic	96
190	E.2.2.3	communication of integrity relevant data - protection strength level normal	96
191	E.2.2.4	communication of integrity relevant data - protection strength level enhanced	96
192	E.2.2.5	communication of integrity relevant data - protection strength level strong	96
193	E.3	confidentiality protection strength	97
194	E.3.1	[CONF-SSM] Confidentiality protecting persistent storage for confidential data	97
195	E.3.1.1	General	97
196	E.3.1.2	confidential persistent storage - strength level basic	97
197	E.3.1.3	confidential persistent storage - strength level normal	97
198	E.3.1.4	confidential persistent storage - strength level enhanced.....	97
199	E.3.1.5	confidential persistent storage - strength level strong.....	97
200	E.3.2	[CONF-COM] Communication of confidential data.....	97
201	E.3.2.1	General	97
202	E.3.2.2	authentication - strength level strong.....	97
203	E.3.2.3	communication of confidential data - protection strength level normal	97
204	E.3.2.4	communication of confidential data - protection strength level enhanced.....	98
205	E.3.2.5	communication of confidential data - protection strength level strong.....	98
206	Annex F (informative):	Relationship between the present document and the covered/not	
207		covered cybersecurity risks.....	98
208	Annex G (informative):	Relationship between the present document and ETSI EN 303 645/	
209		ETSI TS 103 701	102
210			
211			

212 Intellectual Property Rights

213 Essential patents

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

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

223 Trademarks

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

228 **DECT™, PLUGTESTS™, UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its
 229 Members. **3GPP™, LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the
 230 3GPP Organisational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of
 231 the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

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

233 Foreword

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

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

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

243 Once the present document is cited in the Official Journal of the European Union under that Regulation, compliance
 244 with the normative clauses of the present document given in table A.1 confers, within the limits of the scope of the
 245 present document, a presumption of conformity with the corresponding requirements of that Regulation and associated
 246 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

247

Modal verbs terminology

248

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

249

250

251

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

252

253 1 Scope

254 The present document specifies vulnerability handling activities, technical requirements and corresponding assessment
255 criteria for internet connected toys related to cybersecurity. The products with digital elements in scope, thereafter
256 "internet connected toys":

257 • are specified within the "technical description" of the "category of product" number "18." by the Commission
258 Implementing Regulation (EU) 2025/2392 [i.2] as:
259 "Internet connected toys that have social interactive features are products with digital elements that are
260 covered by Directive 2009/48/EC, that communicate on the public Internet, whether directly or via any other
261 equipment, and that have embedded technologies that enable inbound and outbound communication, such as
262 keyboard, microphone, speaker or camera." or "Internet connected toys that have location tracking features are
263 products with digital elements that are covered by Directive 2009/48/EC, that communicate on the public
264 Internet, whether directly or via any other equipment, and that have technologies that enable tracking or
265 inferring of the geographical location of the toy or its user. Where the toy merely detects the proximity of the
266 user or of other toys by using sensing technologies, the toy is not to be considered to have location tracking
267 features." and

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

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

271 2 References

272 2.1 Normative references

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

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

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

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

281 [1] CEN/CLC JT013090:2026 (CEN/CLC prEN 40000-1-3): "Cybersecurity requirements for
282 products with digital elements - Vulnerability Handling".

283 [2] [Agreed Cryptographic Mechanisms](#): "European Union Agency for Cybersecurity, European
284 Cybersecurity Certification Group - Sub-group on Cryptography - Agreed Cryptographic
285 Mechanisms".

286 2.2 Informative references

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

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

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

- 294 [i.1] [Regulation \(EU\) 2024/2847](#): "Regulation (EU) 2024/2847 of the European Parliament and of the
295 Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital
296 elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU)
297 2020/1828 (Cyber Resilience Act)".
- 298 [i.2] [Regulation \(EU\) 2025/2392](#): "Commission Implementing Regulation (EU) 2025/2392 of 28
299 November 2025 on the technical description of the categories of important and critical products
300 with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of
301 the Council".
- 302 [i.3] [Standardisation request M/606 - C\(2025\)618](#): "Commission Implementing decision of 3.2.2025 on
303 a standardisation request to the European Committee for Standardisation (CEN), the European
304 Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications
305 Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU)
306 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal
307 cybersecurity requirements for products with digital elements and amending Regulations (EU) No
308 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)".
- 309 [i.4] CEN/CLC JT013095:2026 (CEN/CLC prEN 40000-1-1): "Cybersecurity requirements for
310 products with digital elements – Vocabulary".
- 311 [i.5] ETSI EN 304 623 vx.x.x: "Cyber Security (CYBER); CRA; Cybersecurity requirements for boot
312 managers".
- 313 [i.6] [ISO/IEC 24760-1:2025](#): "Information security, cybersecurity and privacy protection — A
314 framework for identity management - Part 1: Core concepts and terminology".

315 3 Definition of terms, symbols and abbreviations

316 3.1 Terms

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

319 ARCHITECTURE RELATED TERMS

320 **application software**: software designed to perform specific user- or internet connected toy-oriented functional tasks
321 on a device, operating on top of the core software, and without direct responsibility for hardware initialization or
322 fundamental system control

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

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

326 **architectural component**: self-contained hardware architectural component or software architectural component that is
327 part of the internet connected toy

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

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

332 **hardware architectural component**: self-contained hardware part of the internet connected toy including its associated
333 software architectural component

334 **software architectural component**: self-contained software part of the internet connected toy

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

336 ASSET CATEGORIES

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

338 **data asset:** asset, that is data processed by the internet connected toy

339 **function asset:** asset, that is a function of the internet connected toy

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

- 341 • a function, whose use can impact the availability of other devices, services or networks,
- 342 • a function, whose use can impact the safety or privacy of human entities,
- 343 • a function, which can communicate confidential data,
- 344 • a function, which can communicate integrity relevant data,
- 345 • a function, which can modify integrity relevant data, or
- 346 • a function, which can modify integrity relevant functions

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

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

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

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

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

352 COMMUNICATION TYPES

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

355 EXAMPLE: communication through a virtual-private-network tunnel with a communication partner in a private
356 network

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

359 EXAMPLE: point to point communication via short-range wireless technologies between two communication
360 partners.

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

363 EXAMPLE: direct communication with a chip after modification on a internet connected toy's hardware
364 architectural component

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

366 EXAMPLE: communication via internet

367 **strict local communication:** ingoing/outgoing communication which requires physical presence at the communication
368 partner

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

370 DATA ASSETS

371 **architectural component's position data:** location data describing the position of an architectural component

372 **internet connected toy state data:** data asset that contains internet connected toy state information

373 **audio input data:** data asset that represents audio information captured by the internet connected toy

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

375 EXAMPLE: assignment of privileges to users

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

377 EXAMPLE: passwords, data hashes, message authentication codes, keys used for symmetric or asymmetric
 378 cryptography, (pseudo-)random numbers
 379 **emergency location sharing data:** architectural component's position data that is intended to support in an emergency
 380 situation

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

382 **geofence location data :** location data that describes a region for an architectural component determining the internet
 383 connected toy's behaviour

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

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

386 **social interactive data:** data containing information related to child interactions with social features of the toy or other
 387 entities

388 EXAMPLE: communication data such as speech, text, image and video interaction, user-generated content,
 389 consumed media content such as educational material, music, audiobooks, videos

390 NOTE: refers to all data generated, exchanged or processed through interactive and communicative
 391 functionalities between the child, the connected toy and other participants (such as parents, peers or
 392 online services)

393 **software package:** data asset that contains software intended to be installed on the internet connected toy

394 **video input data:** data asset that represents video information captured by the internet connected toy

395 EXAMPLE: video or picture recordings processed (including storage) on the internet connected toy

396 **DATA RELATED TERMS**

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

399 EXAMPLE: symmetric keys, private keys

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

401 **data:** information in digital form

402 **location data:** data containing geographical information

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

405 EXAMPLE: symmetric keys, private keys

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

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

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

410 **processed data:** data processed by the internet connected toy, including but not limited to capturing, storing,
 411 transmitting, modifying, deleting and presenting data

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

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

414 **FUNCTION ASSETS**

415 **access control mechanism:** internet connected toy function that enforces an authorization policy

416 **audio input function:** internet connected toy function that converts audio signals into data

417 **audio output function:** internet connected toy function that converts data into audio signals

- 418 **authentication mechanism:** internet connected toy function that verifies an entity's claimed identity
- 419 **bootloader function:** internet connected toy function that initiates the execution of other core software at start up.
- 420 **configuration function:** internet connected toy function that allows to change the configuration of internet connected
421 toy's functions
- 422 **connection function:** internet connected toy function that is used for testing or establishing communication capability
423 via machine interface
- 424 **EXAMPLE:** ICMP, DHCP Discovery
- 425 **NOTE:** In this context, establishing communication means communication without user-related data and without
426 authentication of the communication partner for the purpose of establishment of a connection.
- 427 **cryptographic function:** internet connected toy function that performs cryptographic algorithm
- 428 **data backup mechanism:** internet connected toy function that copies data assets to persistent storage of another
429 architectural component or target outside the internet connected toy.
- 430 **data presenting function:** internet connected toy function that grants an entity read access to data or presents data to a
431 user via physical human interface
- 432 **EXAMPLE 1:** Presenting data to a user on a website associated with a RDPS
- 433 **EXAMPLE 2:** Presenting data on a display, controlling indicator lights
- 434 **emergency location function:** internet connected toy function which provides architectural component's position data
435 in case of an emergency
- 436 **factory reset function:** internet connected toy function that removes all user-related data and sets the architectural
437 components in a factory default state, potentially keeping software updates
- 438 **geo fencing notification function:** internet connected toy function which triggers a notification when an architectural
439 component leaves or enters a region defined via geofence location data
- 440 **input sanitization mechanism:** internet connected toy function that scans function input data based on a function
441 specific pattern and removes or alters parts, that can lead to incidents
- 442 **EXAMPLE:** If external data input is amongst others intended to be stored via a database service, escape
443 characters and other database service specific commands (defined by a corresponding function
444 specific pattern) are removed from the external data input, before it is processed by the database
445 service.
- 446 **input validation mechanism:** internet connected toy function that rejects input data if it does not meet an accepted
447 pattern
- 448 **EXAMPLE:** The input is expected to be the users' year of birth. Data type validation is used to ensure the input
449 to be an integer followed by a range validation checking that the input is between 1900 and the
450 current year.
- 451 **location sharing function:** internet connected toy function that shares architectural component's position data
- 452 **logging mechanism:** internet connected toy function that logs events
- 453 **monitoring mechanism:** internet connected toy function that frequently measures functional metrics of the internet
454 connected toy
- 455 **notification mechanism:** internet connected toy function that notifies entities on certain events
- 456 **parental control function:** internet connected toy function that enables parents or guardians to control:
- 457
 - 457 • access rights of children on the internet connected toy,
 - 458 • sources where children can access external content from or
 - 459 • persons that can communicate with the child
- 460 **positioning function:** internet connected toy function that determines an architectural component's position

461 **real-time service or clock:** service or function that provides real time information

462 **sensing function:** internet connected toy function to measure characteristics of its physical operational environment

463 **software package verification mechanism:** internet connected toy function that verifies the integrity and authenticity
464 of software packages

465 **software update mechanism:** internet connected toy function that receives and installs software updates

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

467 **video input function:** internet connected toy function that converts video signals into data

468 **video output function:** internet connected toy function that converts data into video signals

469 FUNCTION RELATED TERMS

470 **authorization policy:** policy that describes the access rights of entities on internet connected toy's data and functions

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

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

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

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

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

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

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

488 NOTE: function output that is an action on the physical operational environment can be performed by a internet
489 connected toy's actuator function.

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

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

494 NOTE: function trigger input provided by the physical operational environment can be received by a internet
495 connected toy's sensing function.

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

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

498 **social interactive function:** internet connected toy function which provides function output as reaction to function
499 trigger input related to social interactions

500 INTERFACES

- 501 **human interface:** interface that is intended to be used by human
- 502 EXAMPLE: PIN pad, touch screen, web interface for user login and user product management
- 503 **interface:** shared boundary across which the internet connected toy exchanges information
- 504 **logical human interface:** interface that is a human interface and a logical interface
- 505 EXAMPLE: web page for remote access
- 506 NOTE: An external client used for remote access providing a logical human interface typically uses a machine
- 507 interface to communicate with the internet connected toy
- 508 **logical interface:** interface that does not exist in hardware and can only be used by using another device or a physical
- 509 interface of a internet connected toy
- 510 **machine interface:** interface that is intended to be used for machine-to-machine communication
- 511 EXAMPLE: Interfaces for USB/Bluetooth®/Ethernet/Wi-Fi®/DECT/DECT-2020 NR or debug ports
- 512 accessible from outside the internet connected toy
- 513 **physical human interface:** interface that is a human interface and a physical interface
- 514 EXAMPLE: keypad, display, biometric reader, microphone, loudspeaker, (video) camera, touchscreen
- 515 **physical interface:** interface that is part of the hardware of a internet connected toy
- 516 EXAMPLE: USB/RJ45/JTAG ports, microSD/SIM card slot
- 517 **OPERATIONAL ENVIRONMENTS**
- 518 **confined operational environment:** physical operational environment, where the geographical location is confined to a
- 519 specific area
- 520 **fully controlled physical operational environment:** physical operational environment, where physical access is fully
- 521 controlled by the guardian or trusted persons
- 522 EXAMPLE: private house or apartment
- 523 **logical operational environment:** operational environment describing the accessibility via logical interfaces
- 524 **mobile operational environment:** physical operational environment, where the geographical location is changing
- 525 during operation and not confined to a specific area
- 526 NOTE: Physical operational environment of smartphones and wearables
- 527 **operational environment:** System used to model to likelihood of incidents depending on the physical operational
- 528 environment of the internet connected toy, or parts of it, and the logical operational environment of the relevant logical
- 529 interfaces.
- 530 **partially controlled physical operational environment:** physical operational environment, that is not a fully
- 531 controlled physical operational environment and either under the control of a limited set of persons or located in an area
- 532 where untrusted physical access is suspicious
- 533 EXAMPLE: Shared area in a house with different apartments or private property where public access is not
- 534 intended.
- 535 **physical operational environment:** operational environment determining the physical accessibility of an architectural
- 536 component
- 537 **stationary operational environment:** physical operational environment, where the geographical location is fixed
- 538 **uncontrolled physical operational environment:** physical operational environment, where physical access control on
- 539 arbitrary untrusted entities cannot be ensured for prolonged time periods and where untrusted physical access is not
- 540 necessarily suspicious
- 541 EXAMPLE: Areas intended for public access
- 542 **USERS**
- 543 **child:** human entity under 14 years of age
- 544 **guardian:** natural or legal entity with responsibility for the child

545 NOTE: This includes also parents

546 **user:** natural entity that directly interacts with the internet connected toy including guardian or child

547 NOTE: This includes all natural entities that interact directly with the internet connected toy as the final product,
548 but not 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 COMMUNICATION TYPES

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

566 IMPACT CLASSES

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

598 IMP.FH.Medium function, whose use can cause harm impact class medium
 599 IMP.FH.SP function, whose use can impact the safety or privacy of human entities impact class
 600 IMP.FH.SP.High function, whose use can impact the safety or privacy of human entities impact class high
 601 IMP.FH.SP.Low function, whose use can impact the safety or privacy of human entities impact class low
 602 IMP.FH.SP.Medium function, whose use can impact the safety or privacy of human entities impact class medium
 603 IMP.High impact class high
 604 IMP.INT integrity impact class
 605 IMP.INT.High integrity impact class high
 606 IMP.INT.Low integrity impact class low
 607 IMP.INT.Medium integrity impact class medium
 608 IMP.Low impact class low
 609 IMP.Medium impact class medium

610 INTERFACES

611 IF interface
 612 IF.Any unspecified interface
 613 IF.Human human interface
 614 IF.HumanLogical logical human interface
 615 IF.HumanPhysical physical human interface
 616 IF.Logical logical interface
 617 IF.Machine machine interface
 618 IF.Physical physical interface

619 OPERATIONAL ENVIRONMENTS

620 POE physical operational environment
 621 POE.Any unspecified physical operational environment
 622 POE.Confined confined operational environment
 623 POE.FullyControlled fully controlled physical operational environment
 624 POE.Mobile mobile operational environment
 625 POE.PartiallyControlled partially controlled physical operational environment
 626 POE.Stationary stationary operational environment
 627 POE.Uncontrolled uncontrolled physical operational environment

628 PROTECTION MEASURE STRENGTH LEVEL

629 AUTH.Basic authentication - strength level basic
 630 AUTH.Enhanced authentication - strength level enhanced
 631 AUTH.Normal authentication - strength level normal
 632 AUTH.Strong authentication - strength level strong
 633 CONF.COM.Basic authentication - strength level strong
 634 CONF.COM.Enhanced communication of confidential data - protection strength level enhanced
 635 CONF.COM.Normal communication of confidential data - protection strength level normal
 636 CONF.COM.Strong communication of confidential data - protection strength level strong
 637 CONF.SSM.Basic confidential persistent storage - strength level basic
 638 CONF.SSM.Enhanced confidential persistent storage - strength level enhanced
 639 CONF.SSM.Normal confidential persistent storage - strength level normal
 640 CONF.SSM.Strong confidential persistent storage - strength level strong
 641 INT.COM.Basic communication of integrity relevant data - protection strength level basic
 642 INT.COM.Enhanced communication of integrity relevant data - protection strength level enhanced
 643 INT.COM.Normal communication of integrity relevant data - protection strength level normal
 644 INT.COM.Strong communication of integrity relevant data - protection strength level strong
 645 INT.SW.VER.Basic software package integrity verification - strength level basic
 646 INT.SW.VER.Enhanced software package integrity verification - strength level enhanced
 647 INT.SW.VER.Normal software package integrity verification - strength level normal
 648 INT.SW.VER.Strong software package integrity verification - strength level strong
 649 N/A not applicable

650 4 Product context

651 4.1 Product functions

652 4.1.1 Essential Functions

653 The present document addresses the following essential functionalities of internet connected toy:

- 654 • **social interactive functions** that might make use of the following functions:
 - 655 - audio input function
 - 656 - video input function
 - 657 - audio output function
 - 658 - video output function
 - 659 - internet connected toy function which can communicate internet connected toy data
 - 660 - internet connected toy function which can modify internet connected toy data
- 661 • positioning functions
- 662 • location sharing functions
- 663 • emergency location functions
- 664 • geo fencing notification functions
- 665 • parental control functions

666 4.1.2 Supporting functions

667 The present document addresses the following supporting functionalities of internet connected toy:

- 668 • configuration function
- 669 • software update mechanism
- 670 • monitoring mechanism
- 671 • notification mechanism
- 672 • logging mechanism
- 673 • access control mechanism
- 674 • authentication mechanism
- 675 • factory reset function
- 676 • integrity protecting communication mechanism
- 677 • confidentiality protecting communication mechanism
- 678 • integrity protecting secure storage mechanism
- 679 • confidentiality protecting secure storage mechanism
- 680 • deletion mechanism
- 681 • onboarding mechanism

- 682 • input sanitization mechanism
- 683 • input validation mechanism
- 684 • software package verification mechanism
- 685 • bootloader function
- 686 • time service or function
- 687 • real-time service or clock
- 688 • cryptographic function
- 689 • data backup mechanism

690 4.1.3 Data assets

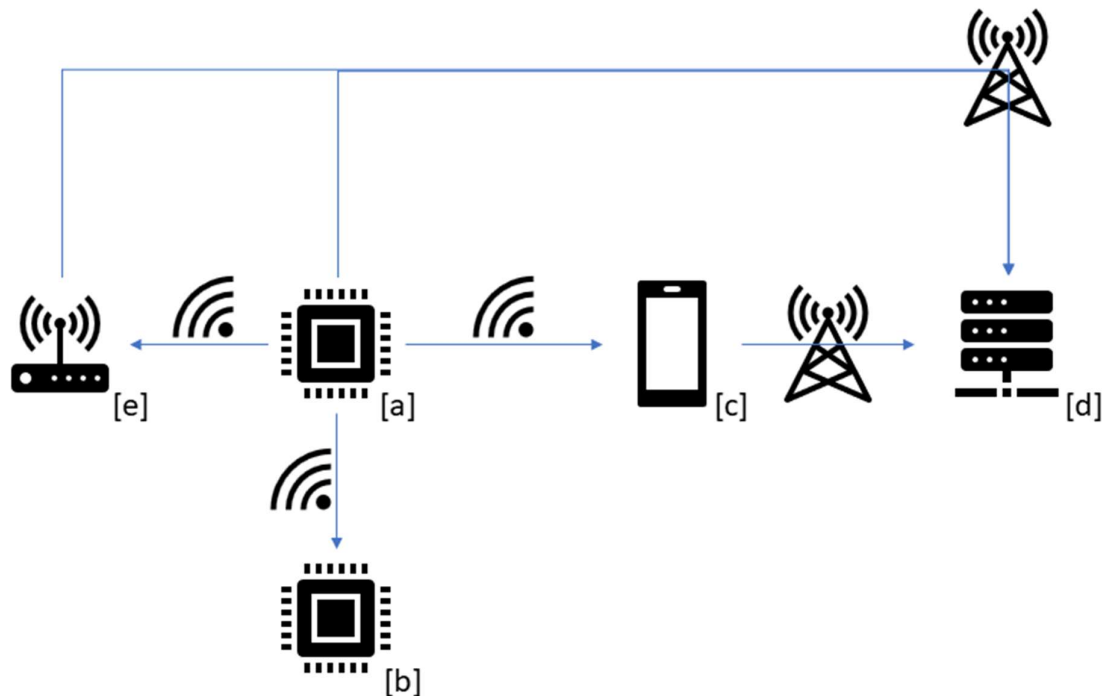
691 The essential and supporting functionalities might process the following data assets:

- 692 • architectural component's position data
- 693 • internet connected toy state data
- 694 • audio input data
- 695 • authorization policy data
- 696 • cryptographic security parameter
- 697 • emergency location sharing data
- 698 • function configuration data
- 699 • geofence location data
- 700 • logging data
- 701 • network status data
- 702 • social interactive data
- 703 • software package
- 704 • video input data

705 4.2 Product Architecture

706 The architecture of a internet connected toy consists of hardware architectural components and/or software architectural
707 components.

708 NOTE: It is possible that a internet connected toy consists of only one hardware architectural component.



709

710

Figure 1: Architectural Components and possible connections between them

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

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

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

720 4.3 Operational Environment

721 The present document addresses the following operational environments of internet connected toy.

722 For the logical operational environment, the following digital communication types are addressed for any architectural
723 component of the internet connected toy:

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

728 The following physical operational environments are addressed for any hardware architectural component of the
729 internet connected toy:

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

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

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

738 4.4 Interfaces

739 The present document addresses the following interfaces of the internet connected toy:

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

744 4.5 Distribution of security functions

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

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

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

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

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

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

758 Situations where the internet connected toy itself does not provide security functions that are required to be used or
759 supported by the internet connected toy and other products with digital elements in the internet connected toy's context
760 do not provide those security functions, 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 internet connected toy:

- 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 functions. The functions covered by the present document are provided in
771 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.AVAL.TIME) of a internet connected toy's function falls under
775 IMP.Low.

776 Use case profile for medium impact functions

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

780 Use case profile for high impact functions

781 The use case profile for high impact functions bundles all use cases addressed by the present document where the
782 maximum impact identified for (IMP.FH, IMP.AVAL.TIME) of a internet connected toy's function falls under
783 IMP.High.

784 4.8 Security Profiles

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

- 787 • security profile for low impact functions
- 788 • security profile for medium impact functions
- 789 • security profile for high impact functions

790

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-PARCONT]	X	X	X
[ACM-FH]	X	X	X
[PARCONT]	X	X	X
[AUM-FH]	X	X	X
[AUTHZ-LP]	X	X	X
[AUTHZ-R]	X	X	X
[AUTHZ-PC]	X	X	X
[INT-SWPCK]	X	X	X
[INT-COM]	X	X	X
[CONF-SSM]	X	X	X
[CONF-COM]	X	X	X
[AVAI-TIME-RECO-POW]	X	X	X
[AVAI-TIME-NETW]	X	X	X
[AVAI-TIME-RECO-NETW]	X	X	X
[AVAI-TIME-OUTA-NOT]		X	X
[AVAI-TIME-PREV-NOT]			X
[AVAI-TIME-NET-PRIO]		X	X
[AVAI-TIME-RES-PRIO]		X	X
[AVAI-TIME-IMP-AMP]		X	X
[AVAI-TIME-DOS-RATE]			X
[AVAI-SUM-SCHEDULE]		X	X
[LAS-INVAL]	X	X	X
[LAS-INSAN]	X	X	X
[LAS-PHY-INF]	X	X	X
[LAS-LOGIC-INF]	X	X	X
[LAS-APP]	X	X	X
[LAS-SBOOT]			X
[DMIN-DJST]	X	X	X
[LOG-LOW]	X		
[LOG-MEDIUM]		X	
[LOG-HIGH]			X
[LOG-TIME]	X	X	
[LOG-TIME-HIGH]			X
[LOG-STORAGE]		X	X
[LOG-BACKUP]			X
[USERNOT-NOSECFUC]	X	X	X
[USERNOT-SECREL]	X	X	X
[GUI-SECCONF]	X	X	X
[CRY-SOTA]	X	X	X
[CRY-CCK-PRE-LEN]	X	X	X
[CRY-CCK-GEN]	X	X	X
[CRY-PW-PRE-COM]	X	X	X
[CRY-PW-GEN-COM]	X	X	X
[CRY-PW-USR-COM]	X	X	X

791

5 Requirements specifications

792

5.1 Product's technical requirements specifications

793 5.1.1 Known exploitable vulnerabilities

794 5.1.1.1 [NKEV-MKAV] No known exploitable vulnerabilities

795 In accordance with the vulnerability handling specified in CEN/CLC JT013090:2026 (CEN/CLC prEN 40000-1-3) [1],
796 the internet connected toy shall prior to making available on the market have no insufficiently mitigated known
797 exploitable vulnerabilities.

798 NOTE 1: The known exploitable vulnerabilities that occur after making the internet connected toy available on the
799 market are subject to the vulnerability handling in CEN/CLC JT013090:2026 (CEN/CLC prEN 40000-1-
800 3) [1].

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

803 5.1.1.2 [NKEV-SUM-SUPPORT] Secure software update mechanism

804 The internet connected toy shall support software update mechanisms, that allow to update every part of the internet
805 connected toy's software, except for parts of the internet connected toy's software, that are immutable due to technical
806 reasons.

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

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

811 5.1.1.3 [NKEV-SUM-PROVIDE] Secure software update mechanism for core 812 components

813 All architectural components of the internet connected toy that include core software shall provide software update
814 mechanisms, that allow to update every part of the architectural components software, except for parts of the
815 architectural components software, that are immutable due to security.

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

817 5.1.1.4 [NKEV-SUM-AUTO] Automated security updates

818 Where the internet connected toy has the capability to connect to a public network, the internet connected toy shall
819 support the automated update of its software.

820 5.1.1.5 [NKEV-SUM-NOTIF] Update notifications

821 Where the internet connected toy has the capability to connect to a public network, the internet connected toy shall
822 support the automated notification of its users, when updates of its software are available.

823 5.1.2 Default configuration

824 5.1.2.1 [SDC-AUM-FH] Default configuration of authentication for functions whose 825 use can cause harm

826 The internet connected toy shall by default be configured to use authentication mechanisms that meet

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

829 except for connection functions.

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

831 5.1.2.2 [SDC-SUM-AUTO] Default configuration of automated security updates

832 Where

- 833 • the internet connected toy has the capability to connect to a public network; and
- 834 • no time sensitive function with IMP.AVAI.TIME.High is provided by an architectural component,
- 835 the architectural component shall by default be configured to use automated software update mechanisms for its
- 836 software.

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

838 NOTE 2: The user can decide to turn off the automated security update mechanism and manually perform the

839 update when is more suitable for him.

840 5.1.2.3 [SDC-SUM-NOTIF] Default configuration of update notifications

841 The internet connected toy shall by default be configured to use automated notification of its users, when updates of the

842 internet connected toy's software are available.

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

844 5.1.2.4 [SDC-FRM] Factory reset to restore the default state

845 The internet connected toy shall provide a factory reset mechanism that allows a guardian to restore the default state,

846 including the deletion of all user-related data, installed applications, and configurations deviating from the default state.

847 NOTE 1: It is also possible that the factory reset will delete the installed security updates if these are installed

848 automatically or on request when the device is commissioned again.

849 NOTE 2: ANNEX II 8. d) of Regulation (EU) 2024/2847 [i.1] contains legal obligations on how users of the

850 internet connected toy are informed about secure decommissioning of the internet connected toy.

851 5.1.2.5 [SDC-PARCONT] Default configuration for parental control

852 The internet connected toy shall by default be configured to:

- 853 • deny children access to security relevant configuration function,
- 854 • restrict the sources where children can access external content from to trusted sources, and
- 855 • restrict entities that can communicate with the child to trusted entities

856 EXAMPLE 1: The internet connected toy is used by the child without any prior configuration by a guardian.

857 Access to communication with others and external data is not possible and cannot be enabled by

858 the child.

859 EXAMPLE 2: The internet connected toy is initially configured by the guardian. The guardian determines which

860 external content the child is allowed to access, with the internet connected toy offering different

861 levels based on the child's age. The trusted entities with which the child is allowed to communicate

862 are also determined by a guardian.

863 NOTE: The requirement [SDC-PARCONT] addresses the default configuration of parental control functions. The

864 support of parental control functions is addressed in [PARCONT]

865 5.1.3 Authentication and access control mechanisms

866 5.1.3.1 [ACM-FH] Access control for functions whose use can cause harm

867 The internet connected toy shall use access control mechanisms to control entities' use of functions whose use can cause

868 harm, where the applicability of this requirement is determined by table 2 except for connection functions.

869 **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		
Att	ck	COM.StrictLocal	POE.FullyControlle	N/A	N/A	applicable[*]
Surf	ace	via IF.Any	d			

			Impact class for function, whose use can cause harm		
			IMP.FH.Low	IMP.FH.Medium	IMP.FH.High
	COM.Local via IF.HumanPhysical	POE.PartiallyControlled	N/A	applicable	applicable
		POE.Mobile	applicable	applicable	applicable
		POE.FullyControlled	N/A	applicable	applicable
	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	

870 For protection measures that are labelled with [*] it is not required that the internet connected toy uses access control
871 mechanisms for its following functions:

- 872 • factory reset function
- 873 • functions configured by parental control function}

874 5.1.3.2 [PARCONT] Support of parental control

875 The internet connected toy shall support parental control functions, covering the parents' or guardians' control of:

- 876 • access rights on the internet connected toy of children,
- 877 • (if the internet connected toy allows children to access external content), the sources where children are
878 allowed to access external content from and
- 879 • (if the internet connected toy allows children to communicate with other persons), the persons that are allowed
880 to communicate with children.

881 5.1.3.3 [AUM-FH] Authentication for functions whose use can cause harm

882 The internet connected toy shall support authentication mechanisms, to authenticate entities using functions whose use
883 can cause harm before generating function output, where

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

886 except for connection functions.

887 **Table 3: Assignment for authentication mechanisms strengths**

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

		Impact class for function, whose use can cause harm		
		IMP.FH.Low	IMP.FH.Medium	IMP.FH.High
COM.Adjacent via IF.Any		AUTH.Normal	AUTH.Normal	AUTH.Enhanced
COM.Public via IF.Any		AUTH.Normal	AUTH.Enhanced	AUTH.Enhanced

888 For protection measures that are labelled with [*] it is not required that the internet connected toy uses authentication
889 mechanisms for its following functions:

- 890 • factory reset function
- 891 • functions configured by parental control function

892 5.1.3.4 [AUTHZ-LP] Least privilege in authorization policies

893 The internet connected toy shall use an authorization policy that only grants permissions that are necessary for the
894 intended purpose.

895 EXAMPLE: The child has no permissions to change security relevant configurations, but the guardian has.

896 NOTE: A internet connected toy whose intended purpose justifies not to differentiate between different user roles,
897 can grant all necessary permissions to the user.

898 5.1.3.5 [AUTHZ-R] Revocability of granted permissions

899 The internet connected toy shall support the revocation of any permission granted by an authorized entity.

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

901 5.1.3.6 [AUTHZ-PC] Authorization policies for parental control

902 The internet connected toy shall use an authorization policy that can differentiate between guardian and child.

903 5.1.4 Integrity protection

904 5.1.4.1 [INT-SWPCK] Software package verification

905 The internet connected toy shall use software package verification mechanisms to verify the integrity and authenticity
906 of software packages prior to installation where the software package verification mechanism's strength levels are
907 specified in clause [E.2.1](#) and where the minimal software package verification mechanism's strength is determined by
908 table [4](#).

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

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

		Highest IMP.INT of the internet connected toy'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

912 5.1.4.2 [INT-COM] Communication of integrity relevant data

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

916
917**Table 5: Assignment of protection mechanisms strength level for the integrity protection of outgoing data and for the integrity verification of incoming data.**

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

918 **5.1.5 Confidentiality protection**919 **5.1.5.1 [CONF-SSM] Confidentiality protecting persistent storage for confidential data**
920

921 The internet connected toy shall use confidentiality protecting secure storage mechanisms for persistently stored
922 confidential data, where the mechanisms' strength are specified in clause [E.3.1](#) and the minimal required mechanisms'
923 strength are determined by table [6](#).

924

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

925 For protection measures labelled with [*], it is not required that the internet connected toy uses confidentiality
926 protecting persistent storage for confidential data:

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

928 **5.1.5.2 [CONF-COM] Communication of confidential data**

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

932
933**Table 7: Assignment of protection mechanisms strength level for the confidentiality of 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

934 5.1.6 Data minimization

935 5.1.6.1 [DMIN-DJST] Documented justification of processed data

936 The internet connected toy shall only process confidential data according to its intended purpose.

937 EXAMPLE: The internet connected toy provides documentation that specifies the conditions under which audio
938 or video data is captured, stored, or transmitted when connected to the intended purpose. The data
939 is processed only in the cases specified in the documentation.

940 5.1.7 Availability protection

941 5.1.7.1 [AVAI-TIME-RECO-POW] Restoration after loss of power

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

944 5.1.7.2 [AVAI-TIME-NETW] Local operation

945 Where network connectivity is not necessary for a time sensitive function to operate, the internet connected toy shall
946 ensure that local operability of this function is supported in case of a loss of network access.

947 5.1.7.3 [AVAI-TIME-RECO-NETW] Restoration after loss of network connection

948 The internet connected toy shall use a mechanism to attempt to reconnect cleanly after a loss of network connection.

949 EXAMPLE: A internet connected toy loses connection to the local network as the network is temporarily
950 unavailable. After recognizing the restored network, the internet connected toy reconnects after a
951 randomized delay to reconnect cleanly.

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

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

956 5.1.7.4 [AVAI-TIME-OUTA-NOT] Notify non-availability

957 Where at least one time sensitive function with IMP.AVAI.TIME.Medium or higher is provided by the internet
958 connected toy, the internet connected toy shall use a mechanism to warn the guardian before or at least during a
959 IMP.AVAI.TIME.Medium or higher function becomes unavailable due to loss of network connection or imminent loss
960 of power.

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

962 NOTE: A mechanism to warn the user cannot ensure that the user receives the warning. For example, a internet
963 connected toy with only local communication connectivity placed in a summer house may run out of
964 battery before the user warning is delivered. However, the user would have been warned when being
965 present before battery exhaustion.

966 5.1.7.5 [AVAI-TIME-PREV-NOT] Notify upcoming limitation

967 Where at least one time sensitive function with IMP.AVAI.TIME.High is provided by the internet connected toy, the
968 internet connected toy shall use a mechanism to notify the guardian before the hardware architectural component
969 restrains the use of power when the internet connected toy recognises low power condition.

970 EXAMPLE: A battery powered internet connected toy recognizes low battery and sends a notification to the
971 guardian.

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

973 5.1.7.6 [AVAI-TIME-NET-PRIO] Network prioritization

974 Where at least one time sensitive function with IMP.AVAI.TIME.Medium or higher with the need of network
975 connectivity for its operation is provided by the internet connected toy, the internet connected toy shall use a
976 mechanism to prioritize its use of network resources in case of a network resource conflict:

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

979 5.1.7.7 [AVAI-TIME-RES-PRIO] Power resource prioritization

980 Where

- 981 • at least one time sensitive function with IMP.AVAI.TIME.Medium or higher is provided by the internet
 982 connected toy; and
 983 • the internet connected toy is intended to be powered by battery,

984 the internet connected toy shall use a mechanism to prioritize use of power in the case of a low power condition:

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

987 5.1.7.8 [AVAI-TIME-IMP-AMP] Amplification control

988 Where at least one function, whose use can impact the availability of other devices, services or networks with
 989 IMP.FH.DSN.Medium or higher is provided by the internet connected toy, the internet connected toy shall use
 990 mechanisms to prevent effective amplification of requests or network traffic of these functions.

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

993 5.1.7.9 [AVAI-TIME-DOS-RATE] Incoming rate limiting

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

997 5.1.7.10 [AVAI-SUM-SCHEDULE] Scheduling of updates

998 Where

- 999 • the internet connected toy has the capability to connect to a public network; and
 1000 • at least one time sensitive function with IMP.AVAI.TIME.Medium or higher is provided by an architectural
 1001 component,

1002 the internet connected toy shall support the scheduling of the application of updates of those architectural components.

1003 5.1.8 Impact minimization

1004 5.1.9 Limit attack surface

1005 5.1.9.1 [LAS-INVAL] Validation of external data input

1006 The internet connected toy shall use input validation mechanisms for all external data input received via:

- 1007 • COM.Local;
 1008 • COM.Adjacent; and
 1009 • COM.Public.

1010 EXAMPLE: If an application expects the input to be an email address, any input that does not conform to the
 1011 format of an e-mail address will be rejected.

1012 NOTE 1: The specific pattern to accept external data input depends amongst others on the manner the external data
 1013 input is intended to be processed. This means that an acceptance pattern for broad purposes (such as
 1014 administration via a "Secure Shell") is typically less specific than an acceptance pattern for a specific
 1015 purpose (such as a measurement value of a specific format to be stored).

1016 NOTE 2: Typically the validation of different parts of the input will happen at different layers. Network layer of the
 1017 operating system verify only information relevant to the network. An application verifies only input that
 1018 is relevant to that application.

1019 5.1.9.2 [LAS-INSAN] Sanitization of external data input

1020 The internet connected toy shall use input sanitization mechanisms at application layer before using external data input,
 1021 where the validation of external data input cannot prevent potential incidents triggered by the external data input.

1022 EXAMPLE: If external data input is amongst others intended to be stored via a database service, escape
 1023 characters and other database service specific commands (defined by a corresponding function
 1024 specific pattern) are removed from the external data input, before it is processed by the database
 1025 service.

1026 5.1.9.3 [LAS-PHY-INF] Only necessary physical interfaces

1027 hardware architectural components shall only provide physical interfaces, that are necessary for the internet connected
 1028 toy's intended purpose.

1029 5.1.9.4 [LAS-LOGIC-INF] Only necessary logical interfaces active by default

1030 The internet connected toy shall by default only provide logical interfaces, that are necessary for its intended purpose.

1031 5.1.9.5 [LAS-APP] Only necessary apps by default

1032 The internet connected toy shall by default only provide installed application software, that are necessary for its
 1033 intended purpose.

1034 5.1.9.6 [LAS-SBOOT] Secure boot

1035 Where at least one function, whose use can cause harm with IMP.FH.High is provided by the internet connected toy and
 1036 the internet connected toy includes hardware architectural components, the hardware architectural components shall use
 1037 a bootloader function that only executes core software at startup, whose integrity and authenticity is verified.

1038 NOTE: The requirement corresponds to the verified boot capability in ETSI EN 304 623 vx.x.x [i.5]

1039 5.1.10 Logging and monitoring mechanisms

1040 5.1.10.1 [LOG-LOW] Events to log for low risk internet connected toy

1041 Where the internet connected toy has a function, whose use can cause harm of impact class low as its highest function
 1042 impact class, the internet connected toy shall support logging mechanisms to create audit events for every:

- 1043 • change of configuration affecting core software;
- 1044 • starts, shutdowns or other changes of operational states of core software;
- 1045 • errors of the core software.

1046 5.1.10.2 [LOG-MEDIUM] Events to log for medium risk internet connected toy

1047 Where the internet connected toy has a function, whose use can cause harm of impact class medium as its highest
 1048 function impact class, the internet connected toy shall use logging mechanisms to create audit events for every:

- 1049 • unsuccessful authentication attempt;
- 1050 • change of configuration affecting core software;
- 1051 • starts, shutdowns or other changes of operational states of core software;

- 1052 • errors of the core software;
- 1053 • unsuccessful attempt of an identity to gain additional privileges;
- 1054 • unsuccessful attempt of an identity to access a data asset or function asset .

1055 5.1.10.3 [LOG-HIGH] Events to log for high risk internet connected toy

1056 Where the internet connected toy has a function, whose use can cause harm of impact class high as its highest function
1057 impact class, the internet connected toy shall use logging mechanisms to create audit events for every:

- 1058 • every authentication attempt;
- 1059 • change of configuration affecting core software;
- 1060 • starts, shutdowns or other changes of operational states of core software;
- 1061 • change of configuration affecting application software whom realize function, whose use can cause harm of
1062 impact class high;
- 1063 • starts, shutdowns or other changes of operational states of application software whom realize function, whose
1064 use can cause harm of impact class high;
- 1065 • errors of the core software;
- 1066 • errors of the application software whom realize function, whose use can cause harm of impact class high;
- 1067 • every attempt of an identity to gain additional privileges;
- 1068 • every attempt of an identity to access a data asset or function asset .

1069 5.1.10.4 [LOG-TIME] Timestamps for logs

1070 Where the internet connected toy does not has a function, whose use can cause harm of impact class high, the internet
1071 connected toy shall use at least a time service or function to include a timestamp in every audit event, created by the
1072 internet connected toy.

1073 5.1.10.5 [LOG-TIME-HIGH] Real-Timestamps for logs

1074 Where the internet connected toy has a function, whose use can cause harm of impact class high as its highest function
1075 impact class, the internet connected toy shall use a real-time service or clock to include a real-time timestamp in every
1076 audit event, created by the internet connected toy.

1077 5.1.10.6 [LOG-STORAGE] Persistently store logfiles

1078 Where the internet connected toy has a function, whose use can cause harm of impact class medium or higher as its
1079 highest function impact class, the internet connected toy shall use integrity protecting secure storage mechanisms to
1080 store every audit event created by the internet connected toy persistently.

1081 5.1.10.7 [LOG-BACKUP] Backup of logfiles

1082 Where the internet connected toy has a function, whose use can cause harm of impact class high as its highest function
1083 impact class, the internet connected toy shall automatically backup its audit events to another device or another part of
1084 the internet connected toy that is in another physical location.

1085 5.1.11 Deletion mechanisms

1086 5.1.11.1 [DLM-PERM] Permanent removal of user-related data

1087 The internet connected toy shall provide at least one deletion mechanism that:

- 1088 • allows a user to permanently remove its user-related data, user-installed applications, including subsets of
1089 those; and

- 1090 • is easy to use.

1091 NOTE: This requirement differs mainly from [SDC-FRM] as [DLM-PERM] allows to delete single data assets.

1092 5.1.12 Other product's technical requirements specifications

1093 5.1.12.1 [USERNOT-NOSECFUC] User notifications on not available security 1094 functions

1095 The internet connected toy shall notify a guardian when security functions that are supposed to be used or supported by
1096 the internet connected toy are not available.

1097 5.1.12.2 [USERNOT-SECREL] Language and representation for security-related user 1098 notifications

1099 Where the internet connected toy is intended to be installed or maintained by a consumer for private usage, the internet
1100 connected toy shall use user notification mechanisms for security-related notifications that:

- 1101 • use a language that is clear, understandable, intelligible, legible and can be easily understood by users for
1102 security-related notifications; and
- 1103 • clearly distinguish the representation of security-related notifications from other notifications.

1104 5.1.12.3 [GUI-SECCONF] Visual representation of security-related configuration via 1105 GUIs

1106 Where the internet connected toy is intended to be installed or maintained by a consumer for private usage, and the
1107 internet connected toy provides a GUI for security-related configuration functionality, the internet connected toy shall
1108 ensure that those GUIs:

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

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

1114 The internet connected toy shall by default only use cryptographic algorithms for cryptographic functions that are

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

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

1119 The internet connected toy shall only provide preinstalled confidential cryptographic keys of key sizes that are

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

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

1124 The internet connected toy shall by default only generate confidential cryptographic keys of key sizes that are

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

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

1127 The internet connected toy shall only provide preinstalled passwords:

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

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

1134 The internet connected toy shall by default only generate passwords:

1135 of minimal recommended password complexity $C_{\{PW,min\}}$ determined by the corresponding authentication

1136 mechanisms' usage according to table 3 and that are random.

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

1138 The internet connected toy shall only use user chosen passwords of minimal recommended password complexity

1139 $C_{\{PW,min\}}$ determined by the corresponding authentication mechanisms' usage according table 3, except for user

1140 chosen passwords where the user explicitly confirms their usage after a warning by the internet connected toy.

1141 5.2 Requirements specifications for vulnerability handling

1142 activities related to the product

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

1144 internet connected toy.

1145 6 Assessing for compliance with requirements

1146 6.1 Assessing for compliance with product's technical

1147 requirements specifications

1148 6.1.1 General

1149 In order to assess the compliance with the requirements listed in clause 5.1 of the present document, the assessment

1150 procedures described in clause 6.1 are to be followed. When performing assessments, the distribution of security

1151 functions (see clause 4.5) are to be considered, including whether the product provides security functions itself,

1152 demands them from other products with digital elements within its context, or supplies them to other products with

1153 digital elements.

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

1155 connected toy) that:

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

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

1159 6.1.2 Known exploitable vulnerabilities

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

1161 **Assessment objective:**

1162 The assessment covers:

- 1163 • a conceptual assessment of [NKEV-SUM-SUPPORT],
- 1164 • a functional completeness assessment on the internet connected toy's capabilities that are addressed by
1165 [NKEV-SUM-SUPPORT]
- 1166 • a functional sufficiency assessment of each software update mechanism used by the internet connected toy to
1167 fulfil [NKEV-SUM-SUPPORT]

1168 based on the default configuration required by clause [5.1.2](#).

1169 **Assessment preparation:**

1170 The following documentation for the internet connected toy shall be complete:

- 1171 • a list of all software architectural components of the SHPSF,
- 1172 • a list of software architectural components declared immutable, including technical justification,
- 1173 • documentation describing all supported software update mechanisms, including:
 - 1174 - their scope, and
 - 1175 - interfaces through which updates can be invoked.

1176 The following test setups shall be prepared:

- 1177 • a test setup that allows to identify software update mechanisms on a sample internet connected toy in default
1178 configuration;
- 1179 • for each software update mechanism, a test setup that allows to perform an update over that software update
1180 mechanism

1181 **Assessment activities:**

1182 The following activities shall be performed:

- 1183 • The internet connected toy's conformity to [NKEV-SUM-SUPPORT] shall be validated based on the
1184 documentation.
- 1185 • The correctness and completeness of the documentation shall be verified by:
 - 1186 - inspecting the internet connected toy to identify software architectural components, e.g. by generating
1187 SBOMs
 - 1188 - whether each identified component is associated with a documented update path.
- 1189 • For each software update mechanism, its correct implementation shall be verified by:
 - 1190 - installing an update over this software update mechanism to update a software architectural component
1191 and
 - 1192 - checking whether the software has changed to the updated software.

1193 **Assignment of verdict:**

1194 The verdict PASS shall be assigned if:

- 1195 • the documentation indicates the internet connected toy's conformity with [NKEV-SUM-SUPPORT]; and
- 1196 • the verification of the correctness and completeness of the documentation was successful; and
- 1197 • the verification of the correct implementation of each software update mechanism was successful.

1198 The verdict FAIL shall be assigned otherwise.

1199 **Supporting Evidence:**

- 1200 • records of the validation of the documentation
- 1201 • descriptions of the performed tests and records of performed tests to verify the correctness and completeness
1202 of the documentation
- 1203 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each
1204 software update mechanism

1205 **6.1.2.2 Assessment criteria for [NKEV-SUM-PROVIDE]**

1206 **Assessment objective:**

1207 The assessment covers:

- 1208 • a conceptual assessment of [NKEV-SUM-PROVIDE],
- 1209 • a functional completeness assessment on the capabilities of the internet connected toy's architectural
1210 components that are addressed by [NKEV-SUM-PROVIDE]
- 1211 • a functional sufficiency assessment of each software update mechanism provided by the internet connected
1212 toy's architectural components to fulfil [NKEV-SUM-PROVIDE]

1213 based on the default configuration required by clause [5.1.2](#).

1214 **Assessment preparation:**

1215 The following documentation for the internet connected toy shall be complete:

- 1216 • a list of all architectural components of the internet connected toy that include core software,
- 1217 • a list of architectural components declared immutable, including technical justification,
- 1218 • documentation describing all provided software update mechanisms, including:
- 1219 - their scope, and
- 1220 - interfaces through which updates can be invoked.

1221 The following test setups shall be prepared:

- 1222 • a test setup that allows to identify software update mechanisms on sample architectural components of the
1223 internet connected toy in default configuration;
- 1224 • for each software update mechanism, a test setup that allows to perform an update over that software update
1225 mechanism

1226 **Assessment activities:**

1227 The following activities shall be performed:

- 1228 • The internet connected toy's conformity to [NKEV-SUM-PROVIDE] shall be validated based on the
1229 documentation.
- 1230 • The correctness and completeness of the documentation shall be verified by:
- 1231 - inspecting the architectural components of the internet connected toy that include core software and
- 1232 - checking whether each identified component is associated with a documented update path.
- 1233 • For each software update mechanism, its correct implementation shall be verified by:
- 1234 - installing an update over this software update mechanism to update a software architectural component
1235 and

1236 - checking whether the software has changed to the updated software.

1237 **Assignment of verdict:**

1238 The verdict PASS shall be assigned if:

- 1239 • the documentation indicates the internet connected toy's conformity with [NKEV-SUM-PROVIDE]; and
- 1240 • the verification of the correctness and completeness of the documentation was successful; and
- 1241 • the verification of the correct implementation of each software update mechanism was successful.

1242 The verdict FAIL shall be assigned otherwise.

1243 **Supporting Evidence:**

- 1244 • records of the validation of the documentation
- 1245 • descriptions of the performed tests and records of performed tests to verify the correctness and completeness
1246 of the documentation
- 1247 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each
1248 software update mechanism

1249 **6.1.2.3 Assessment criteria for [NKEV-SUM-AUTO]**

1250 **Assessment objective:**

1251 The assessment covers:

- 1252 • a conceptual assessment of [NKEV-SUM-AUTO],
- 1253 • a functional sufficiency assessment of each software update mechanism used by the SHPSF to fulfil
1254 [NKEV-SUM-AUTO]

1255 based on the default configuration required by clause [5.1.2](#).

1256 **Assessment preparation:**

1257 The following documentation for the internet connected toy shall be complete:

- 1258 • documentation describing all supported software update mechanism, including:
 - 1259 - their scope,
 - 1260 - interfaces through which updates can be invoked, and
 - 1261 - their capability to perform automatic updates

1262 The following test setups shall be prepared:

- 1263 • for each software update mechanism, a test setup that ensures internet-connectivity and that allows to perform
1264 an automatic update over that software update mechanism

1265 **Assessment activities:**

1266 The following activities shall be performed:

- 1267 • The internet connected toy's conformity to [NKEV-SUM-AUTO] shall be validated based on the
1268 documentation.
- 1269 • For each software update mechanism, its correct implementation shall be verified by:
 - 1270 - installing an automatic update with internet connection over this software update mechanism to update a
1271 software architectural component,

- 1272 - checking whether the product performs the automatic update without human intervention at the product
 1273 or via scheduling the installation under human approval or via triggering the installation under human
 1274 approval, and
- 1275 - checking whether the software version has been updated to a new version.

1276 **Assignment of verdict:**

1277 The verdict PASS shall be assigned if:

- 1278 • the documentation indicates the internet connected toy's conformity with [NKEV-SUM-AUTO] and
- 1279 • the verification of the correct implementation of each software update mechanism was successful.

1280 The verdict FAIL shall be assigned otherwise.

1281 **Supporting Evidence:**

- 1282 • records of the validation of the documentation
- 1283 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each
 1284 software update mechanism

1285 **6.1.2.4 Assessment criteria for [NKEV-SUM-NOTIF]**

1286 **Assessment objective:**

1287 The assessment covers:

- 1288 • a conceptual assessment of [NKEV-SUM-NOTIF],
- 1289 • a functional completeness assessment on the internet connected toy's capabilities that are addressed by
 1290 [NKEV-SUM-NOTIF]
- 1291 • a functional sufficiency assessment of each software update notification mechanism used by the internet
 1292 connected toy to fulfil [NKEV-SUM-NOTIF]

1293 based on the default configuration required by clause [5.1.2](#).

1294 **Assessment preparation:**

1295 The following documentation for the internet connected toy shall be complete:

- 1296 • documentation describing all supported software update notification mechanisms, including:
 - 1297 - how the software update notification is performed, and
 - 1298 - to what extent this software update notification is automated.

1299 The following test setups shall be prepared:

- 1300 • a test setup that allows to identify software update notification mechanisms on a sample internet connected toy
 1301 in default configuration;
- 1302 • for each software update notification mechanism, a test setup that allows to make software updates available
 1303 and therefore to trigger the notification

1304 **Assessment activities:**

1305 The following activities shall be performed:

- 1306 • The internet connected toy's conformity to [NKEV-SUM-NOTIF] shall be validated based on the
 1307 documentation.
- 1308 • The correctness and completeness of the documentation shall be verified by:

- 1309 - inspecting the internet connected toy to identify software update notification mechanisms.
- 1310 • For each software update notification mechanism, its correct implementation shall be verified by:
- 1311 - making a software update available at the source holding security updates and
- 1312 - checking whether the software update notification mechanism automatically notifies the internet
- 1313 connected toy's users that an update of its software is available

1314 **Assignment of verdict:**

1315 The verdict PASS shall be assigned if:

- 1316 • the documentation indicates the internet connected toy's conformity with [NKEV-SUM-NOTIF]; and
- 1317 • the verification of the correctness and completeness of the documentation was successful; and
- 1318 • the verification of the correct implementation of each software update notification mechanism was successful.

1319 The verdict FAIL shall be assigned otherwise.

1320 **Supporting Evidence:**

- 1321 • records of the validation of the documentation
- 1322 • descriptions of the performed tests and records of performed tests to verify the correctness and completeness
- 1323 of the documentation
- 1324 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each
- 1325 software update notification mechanism

1326 **6.1.3 Default configuration**

1327 **6.1.3.1 Assessment criteria for [SDC-AUM-FH]**

1328 **Assessment objective:**

1329 The assessment covers:

- 1330 • a conceptual assessment of [SDC-AUM-FH];
- 1331 • a functional completeness assessment on the internet connected toy capabilities that are addressed by
- 1332 [SDC-AUM-FH];

1333 based on the factory default state.

1334 NOTE: A functional sufficiency assessment of each authentication mechanism used by the internet connected toy to

1335 fulfil [SDC-AUM-FH] is addressed by the assessment of [AUM-FH].

1336 **Assessment preparation:**

1337 The following documentation for the internet connected toy shall be complete:

- 1338 • a list of internet connected toy's functions whose use can cause harm that are enabled in the factory default
- 1339 state or can be activated during initialisation.
- 1340 - the physical operational environment of the architectural component that performs the function;
- 1341 - for each of the function's trigger input possibilities:
- 1342 ▪ the interface and communication type;
- 1343 ▪ a list of corresponding authentication mechanisms including:
- 1344 • the authentication mechanisms' strength;

1345 NOTE: This documentation is a subset of the documentation required for the assessment of [AUM-FH]

1346 The following test setups shall be prepared:

- 1347 • a test setup for identifying functions, their trigger input possibilities and corresponding authentication
- 1348 mechanisms based on a sample internet connected toy in factory default state and after initialisation

1349 **Assessment activities:**

- 1350 • The internet connected toy's conformity to [SDC-AUM-FH] shall be validated based on the documentation.
- 1351 • The correctness and completeness of the documentation shall be verified by:
 - 1352 - inspecting the internet connected toy in factory default state; and
 - 1353 - (if functions whose use can cause harm can be configured during initialisation) performing the
 - 1354 initialisation without providing explicit confirmation of configurations deviating from the minimal
 - 1355 required authentication strength determined by table 3 and inspecting the internet connected toy after
 - 1356 initialisation.

1357 **Assignment of verdict:**

1358 The verdict PASS shall be assigned if:

- 1359 • the documentation indicates the internet connected toy's conformity to [SDC-AUM-FH]; and
- 1360 • the verification of the correctness and completeness of the documentation was successful

1361 The verdict FAIL shall be assigned otherwise.

1362 **Supporting Evidence:**

- 1363 • records of the validation of the documentation;
- 1364 • descriptions of the performed tests and records of performed tests to verify the correctness and completeness
- 1365 of the documentation.

1366 **6.1.3.2 Assessment criteria for [SDC-FRM]**

1367 **Assessment objective:**

1368 The assessment functionally determines whether all user-related data, installed applications, and configurations

1369 deviating from the default state are erased after using the factory reset mechanism.

1370 **Assessment preparation:**

- 1371 • Documentation on how the factory reset mechanism can be accessed.
- 1372 • The internet connected toy shall be set up and some configuration changes shall be created and persistently
- 1373 stored.
- 1374 • Where the internet connected toy supports the storage of user-related data, some user-related data shall be
- 1375 created and persistently stored on the internet connected toy.
- 1376 • Where the internet connected toy supports the installation of applications, some common application for the
- 1377 internet connected toy shall be installed.

1378 NOTE: User-related data also encompasses cryptographic keys, e.g. Wi-Fi® passwords, certificates.

1379 **Assessment activities:**

- 1380 • An authorised entity shall start the factory reset mechanism.
- 1381 • The erasure of user-related data, applications and configurations shall be validated:

1382 - The restoration of the device settings to their default state shall be validated.

1383 • Attempts to access any previous user accounts or data shall be made.

1384 **Assignment of verdict:**

1385 The verdict PASS shall be assigned when all user-related data, installed applications, and configurations deviating from
1386 the default state are erased

1387 The verdict FAIL shall be assigned otherwise.

1388 **Supporting Evidence:**

1389 • Description of the performed test

1390 • All test records of the performed test

1391 6.1.4 Authentication and access control mechanisms

1392 6.1.4.1 Assessment criteria for [ACM-FH]

1393 **Assessment objective:**

1394 The assessment covers:

1395 • a conceptual assessment of [ACM-FH];

1396 • a functional completeness assessment on the internet connected toy capabilities that are addressed by
1397 [ACM-FH];

1398 • a functional sufficiency assessment of each access control mechanism used by the internet connected toy to
1399 fulfil [ACM-FH]

1400 based on the default configuration required by clause [5.1.2](#).

1401 **Assessment preparation:**

1402 The following documentation for the internet connected toy shall be complete:

1403 • a list of internet connected toy's functions whose use can cause harm;

1404 • for each function, whose use can cause harm:

1405 - its impact class impact class for function, whose use can cause harm;

1406 - the physical operational environment of the architectural component that performs the function;

1407 - for each of the function's trigger input possibilities:

1408 ▪ the interface and communication type;

1409 ▪ a list of corresponding access control mechanisms including their default authorization policy.

1410 The following test setups shall be prepared:

1411 • a test setup for identifying functions, their trigger input possibilities and corresponding access control
1412 mechanisms based on a sample internet connected toy in default configuration;

1413 • for each access control mechanism, a test setup that allows privilege escalation attacks from authenticated
1414 entities and unauthorized access attempts of unauthenticated entities.

1415 **Assessment activities:**

1416 • The internet connected toy's conformity to [ACM-FH] shall be validated based on the documentation.

1417 • The correctness and completeness of the documentation shall be verified by:

- 1418 - an inspection of the internet connected toy for functions and related access control mechanisms that are
1419 accessible via physical human interfaces;
- 1420 - a scan of the internet connected toy for functions and related access control mechanisms that are
1421 accessible via logical interfaces.
- 1422 • For each access control mechanism, its correct implementation shall be verified based on attempts to violate
1423 the authorization policy by:
- 1424 - privilege escalation of authenticated entities based on the default authorization policy;
- 1425 - unauthorized usage of function, whose use can cause harm by unauthenticated entities based on the
1426 default authorization policy.

1427 **Assignment of verdict:**

1428 The verdict PASS shall be assigned if:

- 1429 • the documentation indicates the internet connected toy's conformity to [ACM-FH]; and
- 1430 • the verification of the correctness and completeness of the documentation was successful; and
- 1431 • the verification of the correct implementation of each access control mechanism was successful.

1432 The verdict FAIL shall be assigned otherwise.

1433 **Supporting Evidence:**

- 1434 • records of the validation of the documentation;
- 1435 • descriptions of the performed tests and records of performed tests to verify the correctness and completeness
1436 of the documentation;
- 1437 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each
1438 access control mechanism

1439 **6.1.4.2 Assessment criteria for [AUM-FH]**

1440 **Assessment objective:**

1441 The assessment covers:

- 1442 • a conceptual assessment of [AUM-FH];
- 1443 • a functional completeness assessment on the internet connected toy capabilities that are addressed by
1444 [AUM-FH];
- 1445 • a functional sufficiency assessment of each authentication mechanism used by the internet connected toy to
1446 fulfil [AUM-FH]

1447 based on the default configuration required by clause [5.1.2](#).

1448 **Assessment preparation:**

1449 The following documentation for the internet connected toy shall be complete:

- 1450 • a list of internet connected toy's functions whose use can cause harm
- 1451 • for each function, whose use can cause harm:
- 1452 - its impact class impact class for function, whose use can cause harm;
- 1453 - the physical operational environment of the architectural component that performs the function;
- 1454 - for each of the function's trigger input possibilities:

- 1455 ▪ the interface and communication type;
- 1456 ▪ a list of corresponding authentication mechanisms including:
- 1457 • the authentication mechanisms' strength;
- 1458 • the type of authentication factors.

1459 The following test setups shall be prepared:

- 1460 • a test setup for identifying functions, their trigger input possibilities and corresponding authentication mechanisms based on a sample internet connected toy in default configuration;
- 1461
- 1462 • for each authentication mechanism, a test setup defined by the test cases provided in clause [E.1](#) according to the needs determined by its strength and the type of its authentication factors.
- 1463

1464 **Assessment activities:**

- 1465 • The internet connected toy's conformity to [AUM-FH] shall be validated based on the documentation.
- 1466 • The correctness and completeness of the documentation shall be verified by:
- 1467 - an inspection of the internet connected toy for functions and related authentication mechanisms that are accessible via physical human interfaces;
- 1468
- 1469 - a scan of the internet connected toy for functions and related authentication mechanisms that are accessible via logical interfaces.
- 1470
- 1471 • For each authentication mechanism, its correct implementation shall be verified based on the test cases provided in clause [E.1](#) according to the needs determined by its strength and the type of its authentication factors.
- 1472
- 1473

1474 **Assignment of verdict:**

1475 The verdict PASS shall be assigned if:

- 1476 • the documentation indicates the internet connected toy's conformity to [AUM-FH]; and
- 1477 • the verification of the correctness and completeness of the documentation was successful; and
- 1478 • the verification of the correct implementation of each authentication mechanism was successful.

1479 The verdict FAIL shall be assigned otherwise.

1480 **Supporting Evidence:**

- 1481 • records of the validation of the documentation;
- 1482 • descriptions of the performed tests and records of performed tests to verify the correctness and completeness of the documentation;
- 1483
- 1484 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each authentication mechanism.
- 1485

1486 **6.1.4.3 Assessment criteria for [AUTHZ-LP]**

1487 **Assessment objective:**

1488 The assessment covers:

- 1489 • a conceptual assessment of [AUTHZ-LP].

1490 based on the default configuration required by clause [5.1.2](#)

1491 **Assessment preparation:**

1492 The following documentation for the internet connected toy shall be complete:

- 1493 • a description of the authorization policies in default configuration including:
 - 1494 - a list of granted permissions for entities on function, whose use can cause harm and
 - 1495 - for each granted permission, a justification that it is necessary for the intended purpose.

1496 **Assessment activities:**

- 1497 • The internet connected toy's conformity to [AUTHZ-LP] shall be validated based on the documentation.

1498 **Assignment of verdict:**

1499 The verdict PASS shall be assigned if:

- 1500 • the documentation indicates the internet connected toy's conformity to [AUTHZ-LP].

1501 The verdict FAIL shall be assigned otherwise.

1502 **Supporting Evidence:**

- 1503 • records of the validation of the documentation

1504 **6.1.4.4 Assessment criteria for [AUTHZ-R]**

1505 **Assessment objective:**

1506 The assessment covers:

- 1507 • a functional sufficiency assessment to ensure the internet connected toy supports revocation of any granted
1508 permissions.

1509 **Assessment preparation:**

1510 The following documentation for the internet connected toy shall be complete:

- 1511 • a list of mechanisms to grant permissions for entities on function, whose use can cause harm.

1512 The following test setups shall be prepared:

- 1513 • for each mechanism to grant permissions, a test setup for granting and revoking permissions for entities on
1514 function, whose use can cause harm.

1515 **Assessment activities:**

- 1516 • For each mechanism to grant permissions, the revocability of grantable permissions shall be verified by:
 - 1517 - granting permissions to an entity;
 - 1518 - revoking the permissions; and
 - 1519 - attempting use permissions after revocation.

1520 **Assignment of verdict:**

1521 The verdict PASS shall be assigned if:

- 1522 • for each mechanism to grant permissions, access is denied after revocation.

1523 The verdict FAIL shall be assigned otherwise.

1524 **Supporting Evidence:**

- 1525 • descriptions of the performed tests and records of performed tests to verify the correct implementation of
1526 [AUTHZ-R].

1527 **6.1.5 Integrity protection**

1528 **6.1.6 Confidentiality protection**

1529 **6.1.7 Data minimization**

1530 **6.1.7.1 Assessment criteria for [DMIN-DJST]**

1531 **Assessment objective:**

1532 The assessment covers:

- 1533
 - a conceptual assessment of Documented justification of processed data

1534 **Assessment preparation:**

1535 The following documentation for the internet connected toy shall be complete:

- 1536
 - a list of all data assets processed by the internet connected toy whose impact class for confidential internet
- 1537 connected toy data is IMP.CONF.Low or higher;
- 1538
 - for each documented confidential data asset, the associated rationale for its necessity explaining why its
- 1539 processing is necessary for the intended purpose of the internet connected toy.

1540 **Assessment activities:**

- 1541
 - The internet connected toy's conformity to [DMIN-DJST] shall be validated based on the documentation.

1542 **Assignment of verdict:**

1543 The verdict PASS shall be assigned if:

- 1544
 - the documentation indicates the internet connected toy's conformity to [DMIN-DJST];

1545 Otherwise, the verdict FAIL shall be assigned.

1546 **Supporting Evidence:**

- 1547
 - records of the validation of the documentation;

1548 **6.1.8 Availability protection**

1549 **6.1.8.1 Assessment criteria for [AVAI-TIME-RECO-POW]**

1550 **Assessment objective:**

1551 The assessment covers:

- 1552
 - a functional sufficiency assessment of the recovery function interaction with each power supply used by the
- 1553 internet connected toy's hardware architectural components to fulfil [AVAI-TIME-RECO-POW]

1554 based on the default configuration required by clause [5.1.2](#).

1555 **Assessment preparation:**

1556 The following documentation for the internet connected toy shall be complete:

- 1557
 - a list of all internet connected toy's hardware architectural components:
- 1558
 - for each internet connected toy's hardware architectural component:
- 1559
 - a list of all power supplies
- 1560
 - for each power supply:

- 1561 ▪ a description whether the power supply can power the hardware architectural component alone
- 1562 - a list of all functionalities of the internet connected toy that need communication involving the hardware
1563 architectural component:
- 1564 ▪ for each of these functionalities:
- 1565 • a list of interfaces of the internet connected toy, where the connection status of the
1566 necessary communication channels can be read; OR
- 1567 • parameters of the necessary communication channels of the hardware architectural
1568 components in order to externally observe if the connection is active
- 1569 • a list of interfaces of the internet connected toy, where the operational status of the
1570 hardware architectural components can be read:
- 1571 ○ description how the operational status can be implied from the interface
1572 readings.

1573 The following test setups shall be prepared:

- 1574 • the internet connected toy is set up in default configuration
- 1575 • a test setup to:
- 1576 - safely disconnect or disable and reconnect or enable the power supplies of the internet connected toy's
1577 hardware architectural components;
- 1578 - enable access to at least one interfaces of the internet connected toy, where the operational status of the
1579 internet connected toy can be read;
- 1580 - enable access to at least one interfaces of the internet connected toy, where the connection status the
1581 necessary communication channels status of the hardware architectural components can be read;
- 1582 - if the connection status for all necessary communication channels of the hardware architectural
1583 components cannot be read from the internet connected toy:
- 1584 ▪ monitor whether all necessary communication channels of the hardware architectural components
1585 are active.

1586 **Assessment activities:**

1587 The following activities shall be performed for each hardware architectural component:

- 1588 • for every possible order in which the hardware architectural component power supplies can be disconnected or
1589 disabled:
- 1590 - disconnect or disable all power supplies of the hardware architectural component
- 1591 - wait at least 30 s
- 1592 - reconnect or enable the power supplies
- 1593 - monitor the operational status of the internet connected toy
- 1594 - monitor the connection status for all necessary communication channels of the hardware architectural
1595 component
- 1596 - record the order in which the power supplies are disconnect or disable and reconnect or enable
- 1597 - record the time relative to the reconnection or enabling of the last power supply, after which the internet
1598 connected toy indicates, that it is operational and all necessary communication channels are established;
1599 OR

- 1600 - record the time relative to the reconnection or enabling of the last power supply, after which every
 1601 necessary communication channel of the hardware architectural component was active at least once, and
 1602 there is no indication that the internet connected toy has not resumed operation

1603 **Assignment of verdict:**

1604 The verdict PASS shall be assigned if:

- 1605 • the internet connected toy signals resume of operations and establishment of all necessary communication
 1606 channels within one hour after the reconnection or enabling of the last power supply; OR
- 1607 • all necessary communication channels of the hardware architectural components were active at least once, and
 1608 there is no indication that the internet connected toy has not resumed operation within one hour
- 1609 • The verdict FAIL shall be assigned otherwise.

1610 **Supporting Evidence:**

- 1611 • descriptions of the performed tests and records of performed tests

1612 **6.1.8.2 Assessment criteria for [AVAI-TIME-NETW]**

1613 **Assessment objective:**

1614 The assessment covers:

- 1615 • a conceptual assessment of [AVAI-TIME-NETW];
- 1616 • a functional completeness assessment on the internet connected toy capabilities that are addressed by
 1617 [AVAI-TIME-NETW];
- 1618 • a functional sufficiency assessment of each time sensitive function without the need of network connectivity to
 1619 operate used by the internet connected toy to fulfil [AVAI-TIME-NETW]

1620 based on the default configuration required by clause [5.1.2](#).

1621 **Assessment preparation:**

1622 The following documentation for the internet connected toy shall be complete:

- 1623 • a list of all time sensitive function of the internet connected toy:
- 1624 • for each time sensitive function:
 - 1625 - description of the functionalities realised or supported by this function
 - 1626 - list of interfaces necessary for the operation of this function
 - 1627 ▪ for each interface:
 - 1628 ▪ communication types of the interface
- 1629 • a list of interfaces of the internet connected toy, where the status of the architectural component's time
 1630 sensitive function can be read
 - 1631 - description how the status can be implied from the interface readings

1632 The following test setups shall be prepared:

- 1633 • the internet connected toy is set up in default configuration
- 1634 • a test setup to:
 - 1635 - disconnect or disable the public communication of the internet connected toy's architectural components

- 1636 - disconnect or disable the adjacent communication of the internet connected toy's architectural
1637 components
- 1638 - enable access to at least one interfaces of the internet connected toy, where the status of the internet
1639 connected toy's time sensitive function can be read

1640 **Assessment activities:**

1641 The following activities shall be performed:

- 1642 • verify the correctness and completeness of the documentation
- 1643 • repeat the following steps for communication types public communication, adjacent communication and both,
1644 depending on the communication type needed by the functions to be tested:
 - 1645 - disconnect or disable the corresponding communication type of the internet connected toys architectural
1646 component
 - 1647 - wait at least 30 s
 - 1648 - for each time sensitive function which does not need any interface with the corresponding
1649 communication type for its operation
 - 1650 ▪ check whether the function is in operable status
 - 1651 ▪ record the status of the function and the disconnected or disabled communication type
 - 1652 - reconnect or enable the corresponding communication type

1653 **Assignment of verdict:**

1654 The verdict PASS shall be assigned if:

- 1655 • no indication, that the documentation is incorrect or incomplete, are found
- 1656 • all checked time sensitive functions are in operable state

1657 The verdict FAIL shall be assigned otherwise.

1658 **Supporting Evidence:**

- 1659 • descriptions of the performed tests and records of performed tests

1660 **6.1.8.3 Assessment criteria for [AVAI-TIME-RECO-NETW]**

1661 **Assessment objective:**

1662 The assessment covers:

- 1663 • a conceptual assessment of [AVAI-TIME-RECO-NETW]
- 1664 • a functional completeness assessment on the internet connected toy capabilities that are addressed by
1665 [AVAI-TIME-RECO-NETW]
- 1666 • a functional sufficiency assessment of the internet connected toys architectural components recovery after loss
1667 of network connection, to fulfil [AVAI-TIME-RECO-NETW]

1668 based on the default configuration required by clause [5.1.2](#).

1669 **Assessment preparation:**

1670 The following documentation for the internet connected toy shall be complete:

- 1671 • a list of all functions of the internet connected toy that need communication involving the architectural
1672 component

- 1673 - for each of these functions:
- 1674 ▪ list of interfaces involving the architectural component and are necessary for the operation of this
1675 function:
- 1676 • for each interface:
- 1677 ○ communication types of the interface
- 1678 - a list of interfaces of the internet connected toy, where the connection status of the necessary
1679 communication channels can be read; OR
- 1680 - parameters of the necessary communication channel of the architectural component in order to externally
1681 observe if the connection is active

1682 The following test setups shall be prepared:

- 1683 • the internet connected toy is set up in default configuration
- 1684 • a test setup to:
- 1685 - disconnect or disable the public communication of the internet connected toys architectural component
- 1686 - disconnect or disable the adjacent communication of the internet connected toys architectural component
- 1687 - enable access to at least one interfaces of the internet connected toy, where the connection status the
1688 necessary interfaces involving the architectural component and are necessary for the operation of these
1689 functions can be read; OR
- 1690 - if the connection status for all necessary interfaces involving the architectural component and are
1691 necessary for the operation of these functions cannot be read from the internet connected toy:
- 1692 ▪ monitor whether all necessary interfaces involving the architectural component and are necessary
1693 for the operation of these functions

1694 **Assessment activities:**

1695 The following activities shall be performed:

- 1696 • verify the correctness and completeness of the documentation by:
- 1697 - check for undocumented interfaces
- 1698 • repeat the following steps for communication types public communication, adjacent communication and both
1699 at the same time:
- 1700 - disconnect or disable the corresponding communication type of the internet connected toys architectural
1701 component
- 1702 - wait at least 60s
- 1703 - reconnect or enable the corresponding communication type
- 1704 - record the corresponding communication type
- 1705 - for each documented function:
- 1706 ▪ monitor the operational status of the function
- 1707 ▪ for each interface necessary for the operation of this function:
- 1708 • monitor the connection status
- 1709 • record the time relative to the reconnection or enabling of the corresponding
1710 communication type, after which the internet connected toy indicates, that the
1711 interface is reconnected; OR

- 1748 • configure at least one notification mechanism
- 1749 • a test setup to:
 - 1750 - limit the network bandwidth between the internet connected toys architectural component and the
 - 1751 internet connected toys RDPS to the internet
 - 1752 - induce a denial-of-service status on the internet connected toy causing increasing demand on processing
 - 1753 resources
 - 1754 - receive notifications from the internet connected toy

1755 **Assessment activities:**

1756 The following activities shall be performed:

- 1757 • verify the correctness and completeness of the documentation
- 1758 • conceptually verify whether the documented notification mechanisms are suitable to send notifications in case
- 1759 of resource limitations
- 1760 • if at least on time sensitive function needs network connectivity:
 - 1761 - progressively lower the network bandwidth available to the internet connected toys architectural
 - 1762 component
 - 1763 ▪ record any received notifications form the internet connected toy
 - 1764 - progressively higher the intensity of requests to induce a denial-of-service status on the internet
 - 1765 connected toy
 - 1766 ▪ record any received notifications form the internet connected toy

1767 **Assignment of verdict:**

1768 The verdict PASS shall be assigned if:

- 1769 • no indication, that the documentation is incorrect or incomplete, are found; and
- 1770 • the internet connected toy sends notifications according to its configuration in case of non-availability of time
- 1771 sensitive function with IMP.AVAI.TIME.Medium or higher induced by DOS; or
 - 1772 - no time sensitive function with IMP.AVAI.TIME.Medium or higher was non-availability due to DOS;
 - 1773 and
 - 1774 • the internet connected toy sends notifications according to its configuration in case of non-availability of time
 - 1775 sensitive function with IMP.AVAI.TIME.Medium or higher induced by network bandwidth limitation; or
 - 1776 - no time sensitive function with IMP.AVAI.TIME.Medium or higher was non-availability due to network
 - 1777 bandwidth limitation.

1778 The verdict FAIL shall be assigned otherwise.

1779 **Supporting Evidence:**

- 1780 • descriptions of the performed tests and records of performed tests

1781 **6.1.8.5 Assessment criteria for [AVAI-TIME-PREV-NOT]**

1782 **Assessment objective:**

1783 The assessment covers:

- 1784 • a conceptual assessment of [AVAI-TIME-PREV-NOT]

1785 • a functional sufficiency assessment of the internet connected toys notification in case of network resource
1786 restrictions, to fulfil [AVAI-TIME-PREV-NOT]

1787 • a functional sufficiency assessment of the internet connected toys notification in case of DOS, to fulfil
1788 [AVAI-TIME-PREV-NOT]

1789 based on the default configuration required by clause [5.1.2](#).

1790 **Assessment preparation:**

1791 The following documentation for the internet connected toy shall be complete:

- 1792 • a list of all time sensitive functions of the internet connected toy:
 - 1793 - for each of these functions:
 - 1794 ▪ the time sensitive availability impact class
 - 1795 ▪ whether the function needs network connectivity
- 1796 • CPU, memory, power and network resources available to the internet connected toy
- 1797 • demands on CPU, memory, power and network resources for workload consistent with the internet connected
1798 toys intended purpose and reasonably foreseeable use
- 1799 • a list of all notification mechanisms of the internet connected toy:
 - 1800 - description how the notification mechanism can be configured

1801 The following test setups shall be prepared:

- 1802 • the internet connected toy is set up in default configuration
- 1803 • configure at least one notification mechanism
- 1804 • a test setup to:
 - 1805 - read or deduced the status of the time sensitive functions from the internet connected toy
 - 1806 - limit the network bandwidth between the internet connected toys architectural component and the
1807 internet connected toys RDPS to the internet
 - 1808 - induce a DOS status on the internet connected toy causing increasing demand on processing resources
 - 1809 - receive notifications from the internet connected toy

1810 **Assessment activities:**

1811 The following activities shall be performed:

- 1812 • verify the correctness and completeness of the documentation
- 1813 • conceptually verify whether the documented notification mechanisms are suitable to send notifications in case
1814 of resource limitations
- 1815 • if at least on time sensitive function needs network connectivity:
 - 1816 - progressively lower the network bandwidth available to the internet connected toys architectural
1817 component
 - 1818 ▪ record any received notifications form the internet connected toy
 - 1819 - progressively higher the intensity of requests to induce a DOS status on the internet connected toy
 - 1820 ▪ record any received notifications form the internet connected toy

1821 **Assignment of verdict:**

1822 The verdict PASS shall be assigned if:

- 1823 • no indication, that the documentation is incorrect or incomplete, are found; and
- 1824 • the internet connected toy sends notifications according to its configuration in case of resource limitations
1825 induced by DOS; and
- 1826 • the internet connected toy sends notifications according to its configuration in case of network bandwidth
1827 limitation; or
- 1828 - no time sensitive function with IMP.AVAI.TIME.High of the internet connected toy of the internet
1829 connected toy needs network connectivity

1830 The verdict FAIL shall be assigned otherwise.

1831 **Supporting Evidence:**

- 1832 • descriptions of the performed tests and records of performed tests

1833 **6.1.8.6 Assessment criteria for [AVAI-TIME-NET-PRIO]**1834 **Assessment objective:**

1835 The assessment covers:

- 1836 • a conceptual assessment of [AVAI-TIME-NET-PRIO]
- 1837 • a functional sufficiency assessment of the internet connected toys resource prioritization in case of
1838 non-availability induced by network resource restrictions, to fulfil [AVAI-TIME-NET-PRIO]

1839 based on the default configuration required by clause [5.1.2](#).1840 **Assessment preparation:**

1841 The following documentation for the internet connected toy shall be complete:

- 1842 • description how the status of the internet connected toys time sensitive functions can be read or deduced
- 1843 • a list of all time sensitive functions of the internet connected toy:
 - 1844 - for each of these functions:
 - 1845 ▪ the time sensitive availability impact class
 - 1846 ▪ whether the function needs network connectivity
- 1847 • prioritization policy for the time sensitive functions of the internet connected toy in case of network resource
1848 conflict

1849 The following test setups shall be prepared:

- 1850 • the internet connected toy is set up in default configuration
- 1851 • a test setup to:
 - 1852 - read or deduced the status of the time sensitive functions from the internet connected toy
 - 1853 - limit the network bandwidth between the internet connected toys architectural component and the
1854 internet connected toys RDPS to the internet

1855 **Assessment activities:**

1856 The following activities shall be performed:

- 1857 • verify the correctness and completeness of the documentation
- 1858 • conceptually verify the prioritization policy
- 1859 • progressively lower the network bandwidth available to the internet connected toys architectural component
- 1860 - record the status of every time sensitive function

1861 **Assignment of verdict:**

1862 The verdict PASS shall be assigned if:

- 1863 • no indication, that the documentation is incorrect or incomplete, are found; and
- 1864 • the prioritization policy is conceptually valid; and
- 1865 • the prioritization policy is represented by the status of every time sensitive function during network bandwidth
1866 limitation.

1867 The verdict FAIL shall be assigned otherwise.

1868 **Supporting Evidence:**

- 1869 • descriptions of the performed tests and records of performed tests

1870 **6.1.8.7 Assessment criteria for [AVAI-TIME-RES-PRIO]**

1871 **Assessment objective:**

1872 The assessment covers:

- 1873 • a conceptual assessment of [AVAI-TIME-RES-PRIO]
- 1874 • a functional sufficiency assessment of the internet connected toys resource prioritization in case of
1875 non-availability induced by DOS, to fulfil [AVAI-TIME-RES-PRIO]

1876 based on the default configuration required by clause [5.1.2](#).

1877 **Assessment preparation:**

1878 The following documentation for the internet connected toy shall be complete:

- 1879 • description how the status of the internet connected toys time sensitive functions can be read or deduced
- 1880 • a list of all time sensitive functions of the internet connected toy:
 - 1881 - for each of these functions:
 - 1882 ▪ the time sensitive availability impact class
 - 1883 ▪ whether the function needs network connectivity
- 1884 • prioritization policy for the time sensitive functions of the internet connected toy in case of CPU, memory or
1885 power resource conflict

1886 The following test setups shall be prepared:

- 1887 • the internet connected toy is set up in default configuration
- 1888 • a test setup to:
 - 1889 - read or deduced the status of the time sensitive functions from the internet connected toy
 - 1890 - induce a DOS status on the internet connected toy causing increasing demand on processing resources

1891 **Assessment activities:**

1892 The following activities shall be performed:

- 1893 • verify the correctness and completeness of the documentation
- 1894 • conceptually verify the prioritization policy
- 1895 • progressively higher the intensity of requests to induce a DOS status on the internet connected toy
- 1896 - record the status of every time sensitive function

1897 **Assignment of verdict:**

1898 The verdict PASS shall be assigned if:

- 1899 • no indication, that the documentation is incorrect or incomplete, are found; and
- 1900 • the prioritization policy is conceptually valid; and
- 1901 • every time sensitive function:
 - 1902 - the status of the function is in accordance with the prioritization policy during DOS.

1903 The verdict FAIL shall be assigned otherwise.

1904 **Supporting Evidence:**

- 1905 • descriptions of the performed tests and records of performed tests

1906 **6.1.8.8 Assessment criteria for [AVAI-TIME-IMP-AMP]**

1907 **Assessment objective:**

1908 The assessment covers:

- 1909 • a conceptual assessment of [AVAI-TIME-NET-PRIO]
- 1910 • a functional sufficiency assessment of the internet connected toys network amplification, to fulfil
- 1911 [AVAI-TIME-NET-PRIO]

1912 based on the default configuration required by clause [5.1.2](#).

1913 **Assessment preparation:**

1914 The following documentation for the internet connected toy shall be complete:

- 1915 • a list of all function, whose use can impact the availability of other devices, services or networks of the
- 1916 internet connected toy:
 - 1917 - for each of these functions:
 - 1918 ▪ the function, whose use can impact the availability of other devices, services or networks impact
 - 1919 class
 - 1920 ▪ a list of all used interfaces

1921 The following test setups shall be prepared:

- 1922 • the internet connected toy is set up in default configuration
- 1923 • a test setup to:
 - 1924 - execute amplification attacks against the internet connected toy
 - 1925 - measure the affective amplification of network traffic caused by the internet connected toy

1926 **Assessment activities:**

1927 The following activities shall be performed:

- 1928 • verify the correctness and completeness of the documentation
- 1929 • for every function, whose use can impact the availability of other devices, services or networks with
1930 IMP.FH.DSN.Medium or higher:
- 1931 - progressively increase the intensity of an amplification attack against this function
- 1932 - measure the affective amplification of network traffic

1933 **Assignment of verdict:**

1934 The verdict PASS shall be assigned if:

- 1935 • no indication, that the documentation is incorrect or incomplete, are found; and
- 1936 • for every function, whose use can impact the availability of other devices, services or networks with
1937 IMP.FH.DSN.Medium or higher:
- 1938 - the affective amplification of network traffic is not higher than 10

1939 The verdict FAIL shall be assigned otherwise.

1940 **Supporting Evidence:**

- 1941 • descriptions of the performed tests and records of performed tests

1942 6.1.8.9 Assessment criteria for [AVAI-TIME-DOS-RATE]

1943 **Assessment objective:**

1944 The assessment covers:

- 1945 • a conceptual assessment of [AVAI-TIME-DOS-RATE]
- 1946 • a functional sufficiency assessment of the internet connected toys network rate limiting, to fulfil
1947 [AVAI-TIME-DOS-RATE]

1948 based on the default configuration required by clause [5.1.2](#).

1949 **Assessment preparation:**

1950 The following documentation for the internet connected toy shall be complete:

- 1951 • a list of all time sensitive function of the internet connected toy:
- 1952 - for each of these functions:
- 1953 ▪ the time sensitive availability impact class
- 1954 ▪ a list of all used interfaces
- 1955 • a list of all machine interface provided by the internet connected toy
- 1956 • rate limiting policy for the internet connected toy

1957 The following test setups shall be prepared:

- 1958 • the internet connected toy is set up in default configuration
- 1959 • a test setup to:
- 1960 - induce a DOS status on the internet connected toy causing increasing demand on processing resources
- 1961 - check the status of all time sensitive function with IMP.AVAI.TIME.High

1962 **Assessment activities:**

1963 The following activities shall be performed:

- 1964 • verify the correctness and completeness of the documentation
- 1965 • progressively higher the intensity of requests to induce a DOS status on the internet connected toy
- 1966 - record the status of every time sensitive function with IMP.AVAI.TIME.High

1967 **Assignment of verdict:**

1968 The verdict PASS shall be assigned if:

- 1969 • no indication, that the documentation is incorrect or incomplete, are found; and
- 1970 • the rate limiting policy is conceptually valid; and
- 1971 • for every time sensitive function with IMP.AVAI.TIME.High or higher:
 - 1972 - the status of the function is in accordance with the rate limiting policy during DOS.

1973 The verdict FAIL shall be assigned otherwise.

1974 **Supporting Evidence:**

- 1975 • descriptions of the performed tests and records of performed tests

1976 **6.1.8.10 Assessment criteria for [AVAI-SUM-SCHEDULE]**

1977 **Assessment objective:**

1978 The assessment covers:

- 1979 • a conceptual assessment of [AVAI-SUM-SCHEDULE]
- 1980 • a functional sufficiency assessment of the internet connected toys notification in case of non-availability
- 1981 induced by DOS, to fulfil [AVAI-TIME-PREV-NOT]

1982 based on the default configuration required by clause [5.1.2](#).

1983 **Assessment preparation:**

1984 The following documentation for the internet connected toy shall be complete:

- 1985 • a list of all time sensitive functions of the internet connected toy:
 - 1986 - for each of these functions:
 - 1987 ▪ the time sensitive availability impact class
- 1988 • a list of all software update mechanisms of the internet connected toy:
 - 1989 - for each of these mechanisms:
 - 1990 ▪ whether this mechanism can effect at least one time sensitive function with
 - 1991 IMP.AVAI.TIME.Medium or higher
 - 1992 ▪ description how the software update mechanism can be configured

1993 The following test setups shall be prepared:

- 1994 • the internet connected toy is set up in default configuration

1995 **Assessment activities:**

1996 The following activities shall be performed:

- 1997
- verify the correctness and completeness of the documentation
- 1998
- for every software update mechanism that can effect at least one time sensitive function with IMP.AVAI.TIME.Medium or higher:
- 1999
- check whether the application of software updates can be scheduled
- 2000
- record the results
- 2001

2002 **Assignment of verdict:**

2003 The verdict PASS shall be assigned if:

- 2004
- no indication, that the documentation is incorrect or incomplete, are found; and
- 2005
- for every software update mechanism that can effect at least one time sensitive function with IMP.AVAI.TIME.Medium or higher:
- 2006
- the application of software updates can be scheduled
- 2007

2008 The verdict FAIL shall be assigned otherwise.

2009 **Supporting Evidence:**

- 2010
- descriptions of the performed tests and records of performed tests

2011 **6.1.9 Impact minimization**

2012 **6.1.10 Limit attack surface**

2013 **6.1.10.1 Assessment criteria for [LAS-SBOOT]**

2014 **Assessment objective:**

2015 The assessment covers:

- 2016
- a conceptual assessment of [LAS-SBOOT]
- 2017
- a functional sufficiency assessment of the bootloader function used by the internet connected toy to fulfil [LAS-SBOOT]
- 2018

2019 based on the default configuration required by clause [5.1.2](#).

2020 **Assessment preparation:**

2021 The following documentation for the internet connected toy shall be complete:

- 2022
- SBOM of the internet connected toy's hardware architectural component including information on which software's integrity and authenticity is protected by the bootloader function
- 2023
- documentation on how the bootloader function verifies the integrity and authenticity of the hardware architectural component's software
- 2024
- 2025

2026 The following test setup shall be prepared:

- 2027
- a test setup for installing integrity and authenticity tampered core software, including a software package including the tampered core software; or
- 2028
- a test setup for tampering the integrity of installed core software;
- 2029

2030 **Assessment activities:**

- 2031
- The internet connected toy's conformity to [LAS-SBOOT] shall be validated based on the documentation.

2032 • The correct implementation of the bootloader function's integrity and authenticity verification of core software
2033 shall be verified based on:

2034 - tampering the integrity and authenticity of installed core software or installing integrity and authenticity
2035 tampered core software; and

2036 - restarting the internet connected toy's hardware architectural component

2037 NOTE: Typical results are:

2038 • the bootloader function refuses to execute the tampered core software (and thus does not execute application
2039 software), and

2040 • either halts, resets, or boots into a secure fallback and

2041 • an error indication is provided (e.g. via a log, an error code, an LED pattern, etc.).

2042 **Assignment of verdict:**

2043 The verdict PASS shall be assigned if:

2044 • the documentation indicates the internet connected toy's conformity to [LAS-SBOOT]; and

2045 • the internet connected toy's hardware architectural component does not execute the modified core software.

2046 Otherwise, the verdict FAIL shall be assigned.

2047 **Supporting Evidence:**

2048 • records of the validation of the documentation

2049 • descriptions of the performed tests and documentation of associated test records that verify the correct
2050 implementation of the bootloader function's integrity and authenticity verification

2051 6.1.11 Logging and monitoring mechanisms

2052 6.1.11.1 Assessment criteria for [LOG-LOW]

2053 **Assessment objective:**

2054 The assessment covers:

2055 • a conceptual assessment of [LOG-LOW]

2056 • a functional sufficiency assessment of logging mechanisms used by the internet connected toy to fulfil
2057 [LOG-LOW]

2058 based on the default configuration required by clause [5.1.2](#).

2059 **Assessment preparation:**

2060 The following documentation for the internet connected toy shall be complete:

2061 • list of all logging mechanisms

2062 • documentation on how the logging mechanisms creates logging data

2063 • documentation for which events logging data are created by which logging mechanism

2064 • documentation on where logging data are stored

2065 The following test setups shall be prepared:

2066 • a test user with the necessary permissions has been set up to trigger the events

2067 • logging mechanism are enabled on the internet connected toy such that at least all the events in the following
2068 point are covered

2069 • a test setup for triggering the following events: - change of configuration affecting core software;

2070 • starts, shutdowns or other changes of operational states of core software;

2071 • errors of the core software

2072 **Assessment activities:**

2073 The following activities shall be performed:

2074 • Verify whether the *list of all logging mechanisms* is complete

2075 • trigger the events listed in *Assessment preparation*

2076 - for each event triggered: verify that logging data is created according to the documentation

2077 **Assignment of verdict:**

2078 The verdict PASS shall be assigned if:

2079 • the *list of all logging mechanisms* is complete; and

2080 • for each event listed in *Assessment preparation* that could be triggered, logging data is created

2081 The verdict FAIL shall be assigned otherwise.

2082 **Supporting Evidence:**

2083 • descriptions of the performed tests and records of performed tests

2084 **6.1.11.2 Assessment criteria for [LOG-MEDIUM]**

2085 **Assessment objective:**

2086 The assessment covers:

2087 • a conceptual assessment of [LOG-MEDIUM]

2088 • a functional sufficiency assessment of logging mechanisms used by the internet connected toy to fulfil
2089 [LOG-MEDIUM]

2090 based on the default configuration required by clause [5.1.2](#).

2091 **Assessment preparation:**

2092 The following documentation for the internet connected toy shall be complete:

2093 • list of all logging mechanisms

2094 • documentation on how the logging mechanisms creates logging data

2095 • documentation for which events logging data are created by which logging mechanism

2096 • documentation on where logging data are stored

2097 The following test setups shall be prepared:

2098 • a test user with the necessary permissions has been set up to trigger the events

2099 • a test setup for triggering the following events: - unsuccessful authentication attempt;

2100 • change of configuration affecting core software;

- 2101 • starts, shutdowns or other changes of operational states of core software;
- 2102 • errors of the core software;
- 2103 • unsuccessful attempt of an identity to gain additional privileges;
- 2104 • unsuccessful attempt of an identity to access a data asset or function asset

2105 **Assessment activities:**

2106 The following activities shall be performed:

- 2107 • Verify whether the *list of all logging mechanisms* is complete
- 2108 • trigger the events listed in *Assessment preparation*
- 2109 - for each event triggered: verify that logging data is created according to the documentation

2110 **Assignment of verdict:**

2111 The verdict PASS shall be assigned if:

- 2112 • the *list of all logging mechanisms* is complete; and
- 2113 • for each event listed in *Assessment preparation* that could be triggered, logging data is created

2114 The verdict FAIL shall be assigned otherwise.

2115 **Supporting Evidence:**

- 2116 • descriptions of the performed tests and records of performed tests

2117 **6.1.11.3 Assessment criteria for [LOG-HIGH]**

2118 **Assessment objective:**

2119 The assessment covers:

- 2120 • a conceptual assessment of [LOG-HIGH]
- 2121 • a functional sufficiency assessment of logging mechanisms used by the internet connected toy to fulfil
- 2122 [LOG-HIGH]

2123 based on the default configuration required by clause [5.1.2](#).

2124 **Assessment preparation:**

2125 The following documentation for the internet connected toy shall be complete:

- 2126 • list of all logging mechanisms
- 2127 • documentation on how the logging mechanisms creates logging data
- 2128 • documentation for which events logging data are created by which logging mechanism
- 2129 • documentation on where logging data are stored

2130 The following test setups shall be prepared:

- 2131 • a test user with the necessary permissions has been set up to trigger the events
- 2132 • a test setup for triggering the following events: - every authentication attempt;
- 2133 • change of configuration affecting core software;
- 2134 • starts, shutdowns or other changes of operational states of core software;

- 2135 • change of configuration affecting application software whom realize function, whose use can cause harm of
- 2136 impact class high;
- 2137 • starts, shutdowns or other changes of operational states of application software whom realize function, whose
- 2138 use can cause harm of impact class high;
- 2139 • errors of the core software;
- 2140 • errors of the application software whom realize function, whose use can cause harm of impact class high;
- 2141 • every attempt of an identity to gain additional privileges;
- 2142 • every attempt of an identity to access a data asset or function asset

2143 **Assessment activities:**

2144 The following activities shall be performed:

- 2145 • Verify whether the *list of all logging mechanisms* is complete
- 2146 • trigger the events listed in *Assessment preparation*
- 2147 - for each event triggered: verify that logging data is created according to the documentation

2148 **Assignment of verdict:**

2149 The verdict PASS shall be assigned if:

- 2150 • the *list of all logging mechanisms* is complete; and
- 2151 • for each event listed in *Assessment preparation* that could be triggered, logging data is created

2152 The verdict FAIL shall be assigned otherwise.

2153 **Supporting Evidence:**

- 2154 • descriptions of the performed tests and records of performed tests

2155 **6.1.11.4 Assessment criteria for [LOG-TIME]**

2156 **Assessment objective:**

2157 The assessment covers:

- 2158 • a functional sufficiency assessment of logging mechanisms used by the internet connected toy to fulfil
- 2159 [LOG-TIME]

2160 based on the default configuration required by clause [5.1.2](#).

2161 **Assessment preparation:**

2162 The following documentation for the internet connected toy shall be complete:

- 2163 • documentation on how the logging mechanisms creates logging data
- 2164 • documentation for which events logging data are created by which logging mechanism
- 2165 • documentation on where logging data are stored
- 2166 • documentation on the time sources and formats used by logging mechanism

2167 The following test setups shall be prepared:

- 2168 • a test user with the necessary permissions has been set up to trigger the events

2169 • logging mechanism are enabled on the internet connected toy such that at least all the events in the following
2170 point are covered

2171 • a test setup for triggering events as described in *Assessment preparation* in clause [6.1.11.1](#) or clause [6.1.11.2](#)

2172 **Assessment activities:**

2173 The following activities shall be performed:

2174 • trigger the events listed in *Assessment preparation* and note the order and approximate time

2175 - for each event triggered: verify that the logging data contains a timestamp

2176 • for all events triggered: verify that the order and relative times, in which the events where triggered, is
2177 represented by the logging data

2178 **Assignment of verdict:**

2179 The verdict PASS shall be assigned if:

2180 • the *list of all logging mechanisms* is complete; and

2181 • for each event listed in *Assessment preparation* that could be triggered, the logging data includes a timestamp;
2182 and

2183 • the order and relative times, in which the events where triggered, is represented by the logging data

2184 The verdict FAIL shall be assigned otherwise.

2185 **Supporting Evidence:**

2186 • descriptions of the performed tests and records of performed tests

2187 **6.1.11.5 Assessment criteria for [LOG-TIME-HIGH]**

2188 **Assessment objective:**

2189 The assessment covers:

2190 • a conceptual assessment of [LOG-TIME-HIGH]

2191 • a functional sufficiency assessment of logging mechanisms used by the internet connected toy to fulfil
2192 [LOG-TIME-HIGH]

2193 based on the default configuration required by clause [5.1.2](#).

2194 **Assessment preparation:**

2195 The following documentation for the internet connected toy shall be complete:

2196 • documentation on how the logging mechanisms creates logging data

2197 • documentation for which events logging data are created by which logging mechanism

2198 • documentation on where logging data are stored

2199 • documentation on the time sources and formats used by logging mechanism

2200 The following test setups shall be prepared:

2201 • a test user with the necessary permissions has been set up to trigger the events

2202 • logging mechanism are enabled on the internet connected toy such that at least all the events in the following
2203 point are covered

2204 • a test setup for triggering events as described in *Assessment preparation* in clause [6.1.11.3](#)

2205 **Assessment activities:**

2206 The following activities shall be performed:

- 2207 • Verify whether the documented time sources are able to produce real time data
- 2208 • trigger the events listed in *Assessment preparation* and note the time
- 2209 - for each event triggered: verify that the logging data contains a timestamp which represents the time, the
- 2210 event was triggered

2211 **Assignment of verdict:**

2212 The verdict PASS shall be assigned if:

- 2213 • the *list of all logging mechanisms* is complete; and
- 2214 • for each event listed in *Assessment preparation* that could be triggered, the logging data includes a timestamp
- 2215 which represents the time, the event was triggered

2216 The verdict FAIL shall be assigned otherwise.

2217 **Supporting Evidence:**

- 2218 • descriptions of the performed tests and records of performed tests

2219 **6.1.11.6 Assessment criteria for [LOG-STORAGE]**

2220 **Assessment objective:**

2221 The assessment covers:

- 2222 • a functional sufficiency assessment of integrity protecting secure storage mechanisms used by the internet
- 2223 connected toy to fulfil [LOG-STORAGE]

2224 based on the default configuration required by clause [5.1.2](#).

2225 **Assessment preparation:**

2226 The following documentation for the internet connected toy shall be complete:

- 2227 • documentation on how the logging mechanisms creates logging data
- 2228 • documentation for which events logging data are created by which logging mechanism
- 2229 • documentation on where logging data are stored
- 2230 • documentation on which integrity protecting secure storage mechanism are used to store logging data

2231 The following test setups shall be prepared:

- 2232 • a test user with the necessary permissions has been set up to trigger the events
- 2233 • logging mechanism are enabled on the internet connected toy such that at least all the events in the following
- 2234 point are covered
- 2235 • a test setup for triggering events as described in *Assessment preparation* in clause [6.1.11.2](#) or clause [6.1.11.3](#)
- 2236 • a test setup to safely restart the internet connected toy

2237 **Assessment activities:**

2238 The following activities shall be performed:

- 2239 • trigger the events listed in *Assessment preparation*

- 2240 • restart the internet connected toy
- 2241 • verify whether all logging data of the triggered events are still present
- 2242 **Assignment of verdict:**
- 2243 The verdict PASS shall be assigned if:
- 2244 • for each event listed in *Assessment preparation* that could be triggered, the logging data is still present after
- 2245 the internet connected toy was restarted
- 2246 The verdict FAIL shall be assigned otherwise.
- 2247 **Supporting Evidence:**
- 2248 • descriptions of the performed tests and records of performed tests
- 2249 **6.1.11.7 Assessment criteria for [LOG-BACKUP]**
- 2250 **Assessment objective:**
- 2251 The assessment covers:
- 2252 • a conceptual assessment of [LOG-BACKUP]
- 2253 • a functional sufficiency assessment of data backup mechanisms used by the internet connected toy to fulfil
- 2254 [LOG-BACKUP]
- 2255 based on the default configuration required by clause [5.1.2](#).
- 2256 **Assessment preparation:**
- 2257 The following documentation for the internet connected toy shall be complete:
- 2258 • documentation on how the logging mechanisms creates logging data
- 2259 • documentation for which events logging data are created by which logging mechanism
- 2260 • documentation on where logging data are stored
- 2261 • documentation on which data backup mechanism are used to backup logging data
- 2262 • documentation on logging data packed up destinations
- 2263 The following test setups shall be prepared:
- 2264 • a test user with the necessary permissions has been set up to trigger the events
- 2265 • logging mechanism are enabled on the internet connected toy such that at least all the events in the following
- 2266 point are covered
- 2267 • a test setup for triggering events as described in *Assessment preparation* in clause [6.1.11.3](#)
- 2268 • a test setup to access all documented logging data backup destinations
- 2269 **Assessment activities:**
- 2270 The following activities shall be performed:
- 2271 • verify whether the documentation names data backup mechanisms for logging data of all events described in
- 2272 *Assessment preparation*
- 2273 • verify whether the documented destinations, where logging data are packed up to, can store these persistently
- 2274 • trigger the events listed in *Assessment preparation*

- 2275 • wait for the automatic backup cycle for the data backup mechanism used to backup logging data
- 2276 • verify whether all logging data of the triggered events are present on the backup destinations

2277 **Assignment of verdict:**

2278 The verdict PASS shall be assigned if:

- 2279 • all logging data of events described in *Assessment preparation* have at least one data backup mechanism
2280 documented; and
- 2281 • all documented destinations, where logging data are packed up to, can store these persistently; and
- 2282 • all logging data of the triggered events are present on the backup destinations

2283 The verdict FAIL shall be assigned otherwise.

2284 **Supporting Evidence:**

- 2285 • descriptions of the performed tests and records of performed tests

2286 6.1.12 Deletion mechanisms

2287 6.1.12.1 Assessment criteria for [DLM-PERM]

2288 **Assessment objective:**

2289 The assessment covers:

- 2290 • a conceptual assessment of [DLM-PERM],
- 2291 • a functional completeness assessment on the internet connected toy's capabilities that are addressed by
2292 [DLM-PERM], and
- 2293 • a functional sufficiency assessment of each deletion mechanism used by the internet connected toy to fulfil
2294 [DLM-PERM]

2295 based on the default configuration required by clause [5.1.2](#).

2296 **Assessment preparation:**

2297 The following documentation for the internet connected toy shall be complete:

- 2298 • a description of each deletion mechanism, including
 - 2299 - deletion scope (i.e. describing what can be deleted by this mechanism),
 - 2300 - method of deletion (e.g. overwriting, access control, changing pointer address, ...),
 - 2301 - method of user interaction and initiation steps,
 - 2302 - whether confirmation is provided after deletion is performed,
 - 2303 - multi-user handling (describing the user rights to delete other users' data)

2304 The following test setups shall be prepared:

- 2305 • a test setup that allows to identify deletion mechanisms on a sample internet connected toy in default
2306 configuration;
- 2307 • for each deletion mechanism, a test setup that allows to:
 - 2308 - create representative user-related data and install applications,
 - 2309 - access the storage location where data and applications are stored, and

2310 - see the user interaction steps (e.g. menu, dialog, confirmation after deletion)

2311 **Assessment activities:**

2312 The following activities shall be performed:

2313 • The internet connected toy's conformity to [DLM-PERM] shall be validated based on the documentation.

2314 • The correctness and completeness of the documentation shall be verified by checking that all documented
2315 deletion mechanisms are implemented.

2316 - For each deletion mechanism, its correct implementation shall be verified by:

2317 - generating user-related data and installing an application as a user,

2318 - deleting the generated user-related data and the application and

2319 - checking whether the

2320 ▪ user-related data and the application are permanently removed, e.g. by at least checking the storage
2321 location of the user-related data and application before and after deletion,

2322 ▪ deletion mechanism is easy to use with limited technical knowledge,

2323 ▪ user can only delete its own data in multi-user systems, and

2324 ▪ user is provided with clear confirmation of deletion after user-related data or a user-installed
2325 application have been deleted.

2326 • Over all deletion mechanisms, it is to be checked whether all generated sample user-related data and installed
2327 applications can be permanently removed.

2328 **Assignment of verdict:**

2329 The verdict PASS shall be assigned if:

2330 • the documentation indicates the internet connected toy's conformity with [DLM-PERM], and

2331 • the verification of the correctness and completeness of the documentation was successful, and

2332 • the verification of the correct implementation of each deletion mechanism was successful, and

2333 • all deletion mechanisms are able to permanently remove all generated user-related data and user-installed
2334 applications.

2335 The verdict FAIL shall be assigned otherwise.

2336 **Supporting Evidence:**

2337 • records of the validation of the documentation

2338 • descriptions of the performed tests and records of performed tests to verify the correctness and completeness
2339 of the documentation

2340 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each
2341 update mechanism and the ability of the internet connected toy to delete all generated user-related data and
2342 applications

2343 **6.1.13 Other product's technical requirements specifications**

2344 **6.1.13.1 Assessment criteria for [USERNOT-SECREL]**

2345 **Assessment objective:**

2346 The assessment covers:

- 2347 • a conceptual assessment of [USERNOT-SECREL];
- 2348 • a functional sufficiency assessment concerning [USERNOT-SECREL] for each user notification mechanism.

2349 **Assessment preparation:**

2350 The following documentation for the internet connected toy shall be complete:

- 2351 • a list of all used user notification mechanisms that can provide security-related notifications; and
- 2352 • for each used user notification mechanism that can provide security-related notifications, a description on:
 - 2353 - how it ensures that it uses a language that can be easily understood by users; and
 - 2354 - how it distinguishes the representation of security-related notifications from other notifications.

2355 The following test setups shall be prepared:

- 2356 • for each of the internet connected toy's used user notification mechanism that can provide security-related
2357 notifications a test setup for:
 - 2358 - generating security-related notifications; and
 - 2359 - (where other notifications are possible) generating other notifications.

2360 **Assessment activities:**

2361 The internet connected toy's conformity to [USERNOT-SECREL] shall be validated based on the documentation. The
2362 correctness of the implementation shall be verified by inspecting for each used user notification mechanism for
2363 security-related notifications whether:

- 2364 • one security-related notification is clear, understandable, intelligible, legible and can be easily understood by
2365 users; and
- 2366 • (where other notifications are possible), the representation of security-related notifications is clearly
2367 distinguished from other notifications.

2368 **Assignment of verdict:**

2369 The verdict PASS shall be assigned if:

- 2370 • the documentation indicates the internet connected toy's conformity to [USERNOT-SECREL]; and
- 2371 • the verification of the correct implementation of each used user notification mechanism for security-related
2372 notifications was successful.

2373 The verdict FAIL shall be assigned otherwise.

2374 **Supporting Evidence:**

- 2375 • records of the validation of the documentation
- 2376 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each
2377 used user notification mechanism for security-related notifications

2378 **6.1.13.2 Assessment criteria for [GUI-SECCONF]**

2379 **Assessment objective:**

2380 The assessment covers:

- 2381 • a conceptual assessment of [GUI-SECCONF];
- 2382 • a functional sufficiency assessment concerning [GUI-SECCONF] for each internet connected toy's GUI for
2383 security-related configuration functionality.

2384 **Assessment preparation:**

2385 The following documentation for the internet connected toy shall be complete:

- 2386 • a list of GUIs for security-related configuration functionality; and
- 2387 • for each GUI for security-related configuration functionality, a description on:
 - 2388 - how it distinguishes the visual representation of security-related configuration options from other
 - 2389 configuration options; and
 - 2390 - how it ensures that it uses a language for communicating the security-related consequences of changing a
 - 2391 security-related configuration option that can be easily understood by users; and
 - 2392 - how it clearly highlights visually when changes to security-related configuration are made by a user.

2393 The following test setups shall be prepared:

- 2394 • a test setup for accessing each internet connected toy's GUI for security-related configuration functionality.

2395 **Assessment activities:**

2396 The internet connected toy's conformity to [GUI-SECCONF] shall be validated based on the documentation. The
 2397 correctness of the implementation shall be verified by inspecting for each internet connected toy's GUI for
 2398 security-related configuration functionality whether:

- 2399 • the visual representation of security-related configuration options is clearly visual distinguished from other
 2400 configuration options; and
- 2401 • the consequences of one security-related configuration option is communicated in a clear, understandable,
 2402 intelligible, legible manner and can be easily understood by users; and
- 2403 • the change of one security-related configuration is clearly highlighted visually.

2404 **Assignment of verdict:**

2405 The verdict PASS shall be assigned if:

- 2406 • the documentation indicates the internet connected toy's conformity to [GUI-SECCONF]; and
- 2407 • the verification of the correct implementation of each GUI for security-related configuration functionality was
 2408 successful.

2409 The verdict FAIL shall be assigned otherwise.

2410 **Supporting Evidence:**

- 2411 • records of the validation of the documentation
- 2412 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each
 2413 GUI for security-related configuration functionality

2414 6.2 Assessment criteria for vulnerability handling activities 2415 related to the product

2416 The assessment criteria specified in CEN/CLC JT013090:2026 (CEN/CLC prEN 40000-1-3) [1] shall be met for the
 2417 internet connected toy based on the corresponding specified input and output.

2418

2419 Annex A (informative): Relationship between the present
2420 document and the requirements of EU Regulation
2421 2024/2847

2422 **DRAFT ANNEX A - DO NOT CONSIDER THE CONTENT - See identified gaps in Annex F**

2423 The present document has been prepared under the Commission's Standardisation request M/606 - C(2025)618 [i.3] to
2424 provide one voluntary means of conforming to the requirements of Regulation (EU) No 2024/2847 of the European
2425 Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital
2426 elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber
2427 Resilience Act).

2428 Once the present document is cited in the Official Journal of the European Union under that Regulation, compliance
2429 with the normative clauses of the present document given in table 'A.1' confers, within the limits of the scope of the
2430 present document, a presumption of conformity with the corresponding requirements of that Regulation and associated
2431 EFTA regulations.

2432
2433

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

Harmonised Standard ETSI EN 304 633					
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] 5.1.3.3 [AUTHZ-LP] 5.1.3.4 [AUTHZ-R] 5.1.3.5 [AUTHZ-PC] 5.1.3.6 [AVAI-TIME-RECO-POW] 5.1.7.1 [AVAI-TIME-NETW] 5.1.7.2 [AVAI-TIME-RECO-NETW] 5.1.7.3 [AVAI-TIME-OUTA-NOT] 5.1.7.4 [AVAI-TIME-PREV-NOT] 5.1.7.5 [AVAI-TIME-NET-PRIO] 5.1.7.6 [AVAI-TIME-RES-PRIO] 5.1.7.7 [AVAI-TIME-IMP-AMP] 5.1.7.8 [AVAI-TIME-DOS-RATE] 5.1.7.9 [AVAI-SUM-SCHEDULE] 5.1.7.10 [CONF-SSM] 5.1.5.1 [CONF-COM] 5.1.5.2 [CRY-SOTA] 5.1.12.4 [CRY-CCK-PRE-LEN] 5.1.12.5 [CRY-CCK-GEN] 5.1.12.6 [CRY-PW-PRE-COM] 5.1.12.7 [CRY-PW-GEN-COM] 5.1.12.8 [CRY-PW-USR-COM] 5.1.12.9 [DLM-PERM] 5.1.11.1 [DMIN-DJST] 5.1.6.1 [GUI-SECCONF] 5.1.12.3 [INT-SWPCK] 5.1.4.1 [INT-COM] 5.1.4.2 [LAS-INVAL] 5.1.9.1 [LAS-INSAN] 5.1.9.2 [LAS-PHY-INF] 5.1.9.3 [LAS-LOGIC-INF] 5.1.9.4 [LAS-APP] 5.1.9.5 [LAS-SBOOT] 5.1.9.6 [LOG-LOW] 5.1.10.1 [LOG-MEDIUM] 5.1.10.2 [LOG-HIGH] 5.1.10.3 [LOG-TIME] 5.1.10.4 [LOG-TIME-HIGH] 5.1.10.5 [LOG-STORAGE] 5.1.10.6 [LOG-BACKUP] 5.1.10.7 [NKEV-MKAV] 5.1.1.1 [NKEV-SUM-SUPPORT] 5.1.1.2 [NKEV-SUM-PROVIDE] 5.1.1.3 [NKEV-SUM-AUTO] 5.1.1.4 [NKEV-SUM-NOTIF] 5.1.1.5 [PARCONT] 5.1.3.2 [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-PARCONT] 5.1.2.5</p>	U	
---	---	----------------------	--	---	--

Harmonised Standard ETSI EN 304 633					
Requirement				Requirement Conditionality	
No	Description	Requirements of Regulation	Clause(s) of the present document	U/C	Condition
			[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-PARCONT] 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] 5.1.3.3 [AUTHZ-LP] 5.1.3.4 [AUTHZ-R] 5.1.3.5 [AUTHZ-PC] 5.1.3.6 [LOG-MEDIUM] 5.1.10.2 [LOG-HIGH] 5.1.10.3 [PARCONT] 5.1.3.2 [SDC-AUM-FH] 5.1.2.1	U	
6	Products with digital elements protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state-of-the-art mechanisms, and by using other technical means.	Annex I, Part I, (2)(e)	[CONF-SSM] 5.1.5.1 [CONF-COM] 5.1.5.2	U	
7	Products with digital elements protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorized by the user, and report on corruptions.	Annex I, Part I, (2)(f)	[INT-SWPCK] 5.1.4.1 [INT-COM] 5.1.4.2 [LOG-LOW] 5.1.10.1 [LOG-MEDIUM] 5.1.10.2 [LOG-HIGH] 5.1.10.3	U	

Harmonised Standard ETSI EN 304 633					
Requirement				Requirement Conditionality	
No	Description	Requirements of Regulation	Clause(s) of the present document	U/C	Condition
8	Products with digital elements process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimization).	Annex I, Part I, (2)(g)	[DMIN-DJST] 5.1.6.1	U	
9	Products with digital elements protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks.	Annex I, Part I, (2)(h)	[AVAI-TIME-RECO-POW] 5.1.7.1 [AVAI-TIME-NETW] 5.1.7.2 [AVAI-TIME-RECO-NETW] 5.1.7.3 [AVAI-TIME-OUTA-NOT] 5.1.7.4 [AVAI-TIME-PREV-NOT] 5.1.7.5 [AVAI-TIME-NET-PRIO] 5.1.7.6 [AVAI-TIME-RES-PRIO] 5.1.7.7 [AVAI-TIME-DOS-RATE] 5.1.7.9 [AVAI-SUM-SCHEDULE] 5.1.7.10	U	
10	Products with digital elements minimize the negative impact by the products themselves or connected products on the availability of services provided by other products or networks.	Annex I, Part I, (2)(i)	[AVAI-TIME-IMP-AMP] 5.1.7.8	U	
11	Products with digital elements are designed, developed and produced to limit attack surfaces, including external interfaces.	Annex I, Part I, (2)(j)	[LAS-INVAL] 5.1.9.1 [LAS-INSAN] 5.1.9.2 [LAS-PHY-INF] 5.1.9.3 [LAS-LOGIC-INF] 5.1.9.4 [LAS-APP] 5.1.9.5 [LAS-SBOOT] 5.1.9.6	U	
12	Products with digital elements are designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques.	Annex I, Part I, (2)(k)	[AVAI-TIME-RECO-POW] 5.1.7.1 [AVAI-TIME-NET-PRIO] 5.1.7.6 [AVAI-TIME-RES-PRIO] 5.1.7.7	U	
13	Products with digital elements provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user.	Annex I, Part I, (2)(l)	[LOG-LOW] 5.1.10.1 [LOG-MEDIUM] 5.1.10.2 [LOG-HIGH] 5.1.10.3 [LOG-TIME] 5.1.10.4 [LOG-TIME-HIGH] 5.1.10.5 [LOG-STORAGE] 5.1.10.6 [LOG-BACKUP] 5.1.10.7 [NKEV-SUM-NOTIF] 5.1.1.5 [USERNOT-NOSECFUC] 5.1.12.1	U	

Harmonised Standard ETSI EN 304 633					
Requirement				Requirement Conditionality	
No	Description	Requirements of Regulation	Clause(s) of the present document	U/C	Condition
14	Products with digital elements provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.	Annex I, Part I, (2)(m)	[DLM-PERM] 5.1.11.1 [SDC-FRM] 5.1.2.4	U	
15	Vulnerability handling requirements	Annex I, Part II	clause 5.2	U	

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

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

Description

A textual reference to the requirement.

Requirements of Regulation

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

Clause(s) of the present document

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

Requirement Conditionality**U/C**

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

Condition

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

2434 Presumption of conformity stays valid only as long as a reference to the present document is maintained in the list
 2435 published in the Official Journal of the European Union. Users of the present document should consult frequently the
 2436 latest list published in the Official Journal of the European Union.

2437 Other Union legislation may be applicable to the product(s) falling within the scope of the present document.

2438 Annex B (informative): Guidance for the application of the 2439 present document

2440 The following approach can be used (e.g. by manufacturers)

- 2441 • to develop products that are compliant the present document; or
- 2442 • to analyse the compliance of a product to the present document.

2443 The approach is constructed such that it uses parts of an assessment of cybersecurity risks and can be integrated into the
 2444 management of cybersecurity risks.

- 2445 • Step 1 - check if the product is in scope of the present document provided in clause [1](#) by:

2446 - verifying that the product is a internet connected toy as specified within the "technical description" of the
 2447 "category of product" number "18." by Regulation (EU) 2025/2392 [i.2]; and

2448 - identifying the product context by:

- 2449 ▪ identifying the product's architectural components; and
- 2450 ▪ identifying all data processed by the product (data assets); and
- 2451 ▪ identifying all functions provided by the product (function assets); and

- 2452 ▪ identifying the architectural components' operational environments; and
- 2453 ▪ identifying the architectural components' interfaces and communication types; and
- 2454 - verifying that the product is covered within the product context described in clause 4 by:
 - 2455 ▪ verifying that the architectural components of the product are covered within the product
 - 2456 architecture described in clause 4.2; and
 - 2457 ▪ verifying that the data processed by the product and the functions provided by the product are
 - 2458 covered within clause 4.1; and
 - 2459 ▪ verifying that the architectural components' operational environments are covered within
 - 2460 clause 4.3; and
 - 2461 ▪ verifying that the architectural components' interfaces and communication types are covered within
 - 2462 clause 4.4.

2463 NOTE 1: The identification of the items mentioned above can be reused for assessing the compliance
2464 of the product with the requirements in clause 5.

2465 NOTE 2: If a product is a internet connected toy as specified by Regulation (EU) 2025/2392 [i.2] but
2466 is not covered within the product context described in clause 4, it is assumed that the product is not or
2467 not completely covered by the present document. In such cases informing ETSI Technical Committee
2468 Cyber Working Group for EUSR (CYBER-EUSR) via the [Committee Support Staff](#) might help to
2469 address those products in potential revisions of the present document.

- 2470 • Step 2 - identify information to determine risk factors by:
 - 2471 - identifying for each function provided by the product:
 - 2472 ▪ its impact classes according to clause D.2; and
 - 2473 ▪ the architectural components that perform the function; and
 - 2474 ▪ the communication types and the interfaces that can receive corresponding function trigger input;
 - 2475 and
 - 2476 - identifying for each data processed by the product:
 - 2477 ▪ its impact classes according to clause D.1
 - 2478 ▪ the architectural components that persistently store the data; and
 - 2479 ▪ the architectural components that can communicate the data; and
 - 2480 ▪ the communication types and the interfaces over which the data is communicated.

2481 NOTE 3: If data processed by the product or functions provided by the product are not covered
2482 within clause 4.1, clause C.1 can be used to identify impact classes for function and data assets that
2483 are outside the scope of the present document.

- 2484 • Step 3 - identify concrete requirements for and specific security measures/mitigations of the product that
2485 satisfy those requirements by:
 - 2486 - for each requirement in clause 5:
 - 2487 ▪ identifying the requirements applicability by evaluating the requirement's potential preconditions
 - 2488 and exceptions based on the product's properties; and
 - 2489 ▪ (for requirements that include assignment tables) identifying the required protection mechanisms'
 - 2490 strengths (specified in annex E) by evaluating the requirement's assignment table based on the
 - 2491 product's properties determining the attack surface and impact parameters; and
 - 2492 ▪ identifying the specific security measures/mitigations that satisfy the requirement.

2493 NOTE 4: An assignment table can yield multiple mechanisms' strengths from different
2494 circumstances, which all have to be satisfied.

2495 EXAMPLE: Authentication requirements prior to changes of a internet connected toys configuration
2496 are different whether the changes can be made via a web GUI, accessible from adjacent or public
2497 networks, a GUI, accessible from the internet connected toys touchscreen, or a console, accessible be
2498 connecting to a serial port. All of these cases can be simultaneously present on the same internet
2499 connected toy.

2500 • Step 4 - assess the compliance of the product with the requirements in clause [5](#) by:

2501 - for each requirement in clause [5](#), performing the corresponding assessment for compliance described in
2502 clause [6](#) (the functional sufficiency assessments for different protection measures strengths are specified
2503 in annex [E](#)) by:

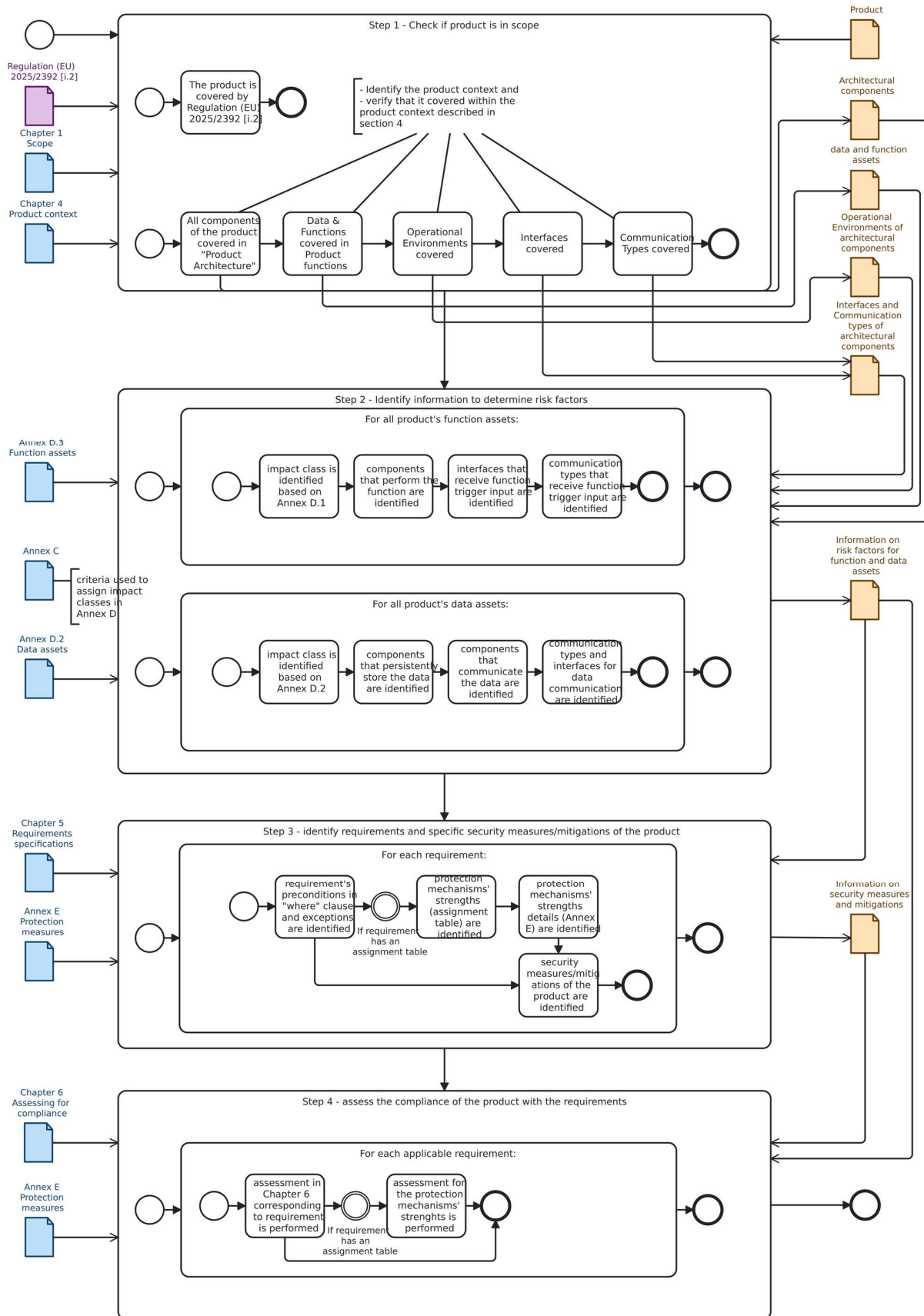
2504 ▪ preparing the assessment for the product; and

2505 ▪ performing the assessment activities for the product; and

2506 ▪ assigning an assessment verdict for the product; and

2507 ▪ generating the supporting evidences for the assessment.

2508 The figure [B.1](#) provides a graphical representation of the guidance for the application of the present document.



2510 **Figure B.1: Graphical representation on guidance for the application of the present document**

2511 **Annex C (informative): Information on the methodology for**
 2512 **the assessment of cybersecurity risks used to develop the**
 2513 **present document**

2514 **This informative annex is intended to provide information on the methodology for the assessment of**
 2515 **cybersecurity risks used to develop the present document.**

2516 **C.1 Guidance for determining impact classes**

2517 **C.1.1 General**

2518 The present document uses the following criteria to determine the impact classes of different specific internet connected
 2519 toy assets provided in annex [D](#).

2520 **C.1.2 confidential data**

2521 **confidentiality impact class low (IMP.CONF.Low):**

2522 The disclosure may lead to:

- 2523 • inconvenient consequences on the user(s); or
- 2524 • additional or increased attack opportunities over a short time and limited to communication types not higher
 2525 than local on the internet connected toy.

2526 **confidentiality impact class medium (IMP.CONF.Medium):**

2527 The disclosure may lead to:

- 2528 • serious impact on the user(s);
- 2529 • additional or increased attack opportunities over a short time on the internet connected toy or a limited number
 2530 of other products; or
- 2531 • additional or increased attack opportunities over a prolonged time limited to non-key-functionalities on the
 2532 internet connected toy.

2533 **confidentiality impact class high (IMP.CONF.High):**

2534 The disclosure may lead to:

- 2535 • significant or even irreversible impact on the user(s) (e.g. personal or financial harm);
- 2536 • additional or increased attack opportunities over a prolonged time on the internet connected toy or a limited
 2537 number of other products; or
- 2538 • additional or increased attack opportunities over a short time on a significant number of other products.

2539 **C.1.3 loss sensitive data**

2540 **loss sensitive availability impact class low (IMP.AVALLOSS.Low):**

2541 The loss may lead to:

- 2542 • inconvenient consequences on the user(s); or
- 2543 • non-availability of non-key-functionalities on the internet connected toy for a short time.

2544 **loss sensitive availability impact class medium (IMP.AVALLOSS.Medium):**

2545 The loss may lead to:

- 2546 • serious impact on the user(s); or
- 2547 • non-availability of key-functionalities of the internet connected toy over a short time; or
- 2548 • non-availability of non-key-functionalities on the internet connected toy for a prolonged time.

2549 **loss sensitive availability impact class high (IMP.AVALLOSS.High):**

2550 The loss may lead to:

- 2551 • significant or even irreversible impact on the user(s) (e.g. personal or financial harm);
- 2552 • non-availability of key-functionalities of the internet connected toy for a prolonged time; or
- 2553 • permanent non-availability of non-key-functionalities of the internet connected toy

2554 C.1.4 time sensitive data and time sensitive function

2555 **time sensitive availability impact class low (IMP.AVAL.TIME.Low):**

2556 The delay of availability may lead to:

- 2557 • non-availability of non-key-functionalities on the internet connected toy for a short time.

2558 **time sensitive availability impact class medium (IMP.AVAL.TIME.Medium):**

2559 The delay of availability may lead to:

- 2560 • non-availability of key-functionalities on the internet connected toy for a short time; or
- 2561 • non-availability of non-key-functionalities on the internet connected toy for a prolonged time.

2562 **time sensitive availability impact class high (IMP.AVAL.TIME.High):**

2563 The delay of availability may lead to:

- 2564 • non-availability of key-functionalities of the internet connected toy for a prolonged time; or
- 2565 • permanent non-availability of non-key-functionalities of the internet connected toy.

2566 C.1.5 integrity relevant data and integrity relevant function

2567 **integrity impact class low (IMP.INT.Low):**

2568 The tampering may lead to:

- 2569 • inconvenient consequences on the user(s);
- 2570 • additional or increased attack opportunities for a short time and limited to communication types not higher
- 2571 than local on the internet connected toy; or
- 2572 • non-availability of non-key-functionalities on the internet connected toy for a short time.

2573 **integrity impact class medium (IMP.INT.Medium):**

2574 The tampering may lead to:

- 2575 • serious impact on the user(s);
- 2576 • additional or increased attack opportunities over a short time on the internet connected toy or a limited number
- 2577 of other products;

2578 • additional or increased attack opportunities over a prolonged time limited to non-key-functionalities on the
2579 internet connected toy; or

2580 • non-availability of key-functionalities on the internet connected toy for a short time; or

2581 • non-availability of non-key-functionalities on the internet connected toy for a prolonged time.

2582 **integrity impact class high (IMP.INT.High):**

2583 The tampering may lead to:

2584 • significant or even irreversible impact on the user(s) (e.g. personal or financial harm);

2585 • additional or increased attack opportunities for a prolonged time on the internet connected toy or a limited
2586 number of other products;

2587 • additional or increased attack opportunities for a short time on a significant number of other products;

2588 • non-availability of key-functionalities of the internet connected toy for a prolonged time; or

2589 • permanent non-availability of non-key-functionalities of the internet connected toy

2590 **Annex D (normative): Relationship between specific data**
 2591 **and functions assets covered by the present document to**
 2592 **impact classes for generic asset categories**

2593 **D.1 Data assets**

2594 **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 internet connected toy data	impact class for integrity relevant internet connected toy data	impact class for time critical availability relevant internet connected toy data	impact class for loss critical availability relevant internet connected toy data
architectural component's position data	IMP.CONF.Medium	IMP.INT.Medium	IMP.AVAI.TIME.Medium	IMP.AVAI.LOSS.Low
emergency location sharing data	IMP.CONF.Low	IMP.INT.Medium	IMP.AVAI.TIME.High	IMP.AVAI.LOSS.Low
geofence location data	IMP.CONF.Low	IMP.INT.Medium	IMP.AVAI.TIME.Medium	IMP.AVAI.LOSS.Low
social interactive data	IMP.CONF.Medium	IMP.INT.Medium	IMP.AVAI.TIME.Low	IMP.AVAI.LOSS.Medium
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
internet connected toy 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 internet connected toy'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)
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

2595 **D.2 Function assets**

2596
2597**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
positioning function	IMP.INT.Medium	IMP.AVAI.TIME.Medium	IMP.FH.Medium
location sharing function	IMP.INT.Medium	IMP.AVAI.TIME.Medium	IMP.FH.Medium
emergency location function	IMP.INT.Medium	IMP.AVAI.TIME.High	IMP.FH.Medium
geo fencing notification function	IMP.INT.Medium	IMP.AVAI.TIME.Medium	IMP.FH.Medium
parental control function	IMP.INT.Medium	IMP.AVAI.TIME.Low	IMP.FH.Medium
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
internet connected toy function which can communicate internet connected toy 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
internet connected toy function which can modify internet connected toy 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

2598
2599

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](#).

2600
2601**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
positioning function	IMP.FH.SP.Medium	no	no	no
location sharing function	IMP.FH.SP.Medium	IMP.FH.DSN.Low	IMP.FH.CCON.Medium	no
emergency location function	IMP.FH.SP.Low	IMP.FH.DSN.Low	IMP.FH.CCON.Low	no
geo fencing notification function	IMP.FH.SP.Medium	IMP.FH.DSN.Low	IMP.FH.CCON.Low	no
parental control function	no	no	IMP.FH.CCON.Low	IMP.FH.MINT.Medium
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
internet connected toy function which can communicate internet connected toy data	no	IMP.FH.DSN.Low	IMP.FH.CCON = IMP.CONF of communicated data	no
connection function	no	IMP.FH.DSN.Medium	no	no
internet connected toy function which can modify internet connected toy 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

2602

Annex E (normative): Protection measures

2603

E.1 authentication mechanism strength

2604

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

2605

E.1.1.1 General

2606

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

2607

2608

2609

E.1.1.2 authentication - strength level basic

2610

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

2611

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

2612

2613

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

2614

2615 E.1.1.3 authentication - strength level normal

2616 The authentication - strength level normal shall protect against the following attack types:

2617 **automated brute force attack:** Brute force attacks on authentication mechanisms based on authentication factors of the
2618 type knowledge, by systematic try out with technical.

2619 **presentation attack:** Presentation attacks on authentication mechanisms based on authentication factors of the type
2620 inherence, using medium effort methods like e.g. photos, cut out masks, audio replays, video replays, AI generated
2621 voices

2622 **automated security token spoofing attack:** Security token spoofing attacks on authentication mechanisms based on
2623 authentication factors of the type possession, by using authentication factors sourced from other uses or self-created,
2624 without using any specific knowledge of the targeted authentication mechanisms.

2625 **replay attack:** An attacker intercepts valid data transmissions and retransmits them to mimic the original
2626 communication partner for accepting an authentication based on the authentication factors of the type knowledge or
2627 possession (e.g. a session token).

2628 **person in the middle attack:** An attacker secretly intercepts and alters the authentication between two parties who
2629 believe they are communicating directly with each other based on the authentication factors of the type knowledge or
2630 possession (e.g. a session token).

2631 E.1.1.4 authentication - strength level enhanced

2632 The authentication - strength level enhanced shall protect against the following attack types:

2633 **targeted presentation attack:** Presentation attacks on authentication mechanisms based on authentication factors of the
2634 type inherence, using enhanced effort methods like e.g. (partial) silicone masks, layered prints

2635 **targeted brute force attack:** Brute force attacks on authentication mechanisms based on authentication factors of the
2636 type knowledge, by systematic try out with technical aids, making use of target specific information.

2637 **targeted security token spoofing attack:** Security token spoofing attacks on authentication mechanisms based on
2638 authentication factors of the type possession, by using authentication factors sourced from devices of the same type as
2639 the internet connected toy or self-created, using specific knowledge of the targeted authentication mechanisms and the
2640 internet connected toy.

2641 **replay attack:** An attacker intercepts valid data transmissions and retransmits them to mimic the original
2642 communication partner for accepting an authentication based on the authentication factors of the type knowledge or
2643 possession (e.g. a session token).

2644 **person in the middle attack:** An attacker secretly intercepts and alters the authentication between two parties who
2645 believe they are communicating directly with each other based on the authentication factors of the type knowledge or
2646 possession (e.g. a session token).

2647 E.1.1.5 authentication - strength level strong

2648 The authentication - strength level strong shall protect against the following attack types:

2649 **elaborate presentation attack:** Presentation attacks on authentication mechanisms based on authentication factors of
2650 the type inherence", using high effort methods like e.g. highly realistic silicone or latex masks, limb replicas, trained
2651 deepfakes

2652 **elaborate brute force attack:** Brute force attacks on authentication mechanisms based on authentication factors of the
2653 type knowledge, by systematic try out with technical aids, making use of target specific information, and unrestricted
2654 duration.

2655 **elaborate security token spoofing attack:** Security token spoofing attacks on authentication mechanisms based on
2656 authentication factors of the type possession, by using authentication factors created or sourced from devices of the
2657 same type as the internet connected toy and modified, specifically for the targeted authentication mechanisms.

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.1.2 Assessment for authentication mechanism strength

2665 E.1.2.1 Assessment criteria regarding the protection against limited presentation 2666 attacks

2667 **Assessment objective:**

2668 The assessment covers functional testing of authentication mechanisms that provide a basic level of protection and use
 2669 authentication factors of the type inherence against limited presentation attacks.

2670 **Assessment preparation:**

- 2671 • the internet connected toy shall be set up in default configuration
- 2672 • a genuine enrolled biometric template in the corresponding authentication mechanism with credential for
 2673 authentication shall be created
- 2674 • at least one interface, where the authentication mechanism is reachable shall be documented

2675 **Assessment activities:**

- 2676 • authentication at the created genuine enrolled biometric template shall be attempted using the correct genuine
 2677 enrolled biometric template identifier, if present, and authentication factors, not belonging to the person who
 2678 set up the account, for at least five times or ten minutes at highest archivable query frequency
- 2679 • the outcome and used authentication factor of each attempt shall be recorded

2680 **Assignment of verdict:**

2681 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts.

2682 The verdict FAIL shall be assigned otherwise.

2683 **Supporting Evidence:**

- 2684 • description of the performed test
- 2685 • all test records of the performed test

2686 E.1.2.2 Assessment criteria regarding the protection against targeted presentation 2687 attacks

2688 **Assessment objective:**

2689 The assessment covers functional testing of authentication mechanisms that provide a enhanced level of protection and
 2690 use authentication factors of the type inherence against targeted presentation attacks.

2691 **Assessment preparation:**

- 2692 • the internet connected toy shall be set up in default configuration
- 2693 • a genuine enrolled biometric template in the corresponding authentication mechanism with credential for
 2694 authentication shall be created
- 2695 • at least one interface, where the authentication mechanism is reachable shall be documented

- 2696 • authentication factors shall be fabricated using common materials and tools as well as readily available source
2697 materials. The fabrication process shall not be longer than *one workday* per authentication factor.

2698 **Assessment activities:**

- 2699 • authentication at the created genuine enrolled biometric template shall be attempted using the correct genuine
2700 enrolled biometric template identifier, if present, and at least two fabricated authentication factors tried at least
2701 five times with slightly different parameters each

- 2702 • the outcome and used authentication factor of each attempt shall be recorded

2703 **Assignment of verdict:**

2704 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts.

2705 The verdict FAIL shall be assigned otherwise.

2706 **Supporting Evidence:**

- 2707 • description of the performed test
2708 • all test records of the performed test

2709 **E.1.2.3 Assessment criteria regarding the protection against elaborate presentation**
2710 **attacks**

2711 **Assessment objective:**

2712 The assessment covers functional testing of authentication mechanisms that provide a high level of protection and use
2713 authentication factors of the type inherence against elaborate presentation attacks.

2714 **Assessment preparation:**

- 2715 • the internet connected toy shall be set up in default configuration
2716 • a genuine enrolled biometric template in the corresponding authentication mechanism with credential for
2717 authentication shall be created
2718 • at least one interface, where the authentication mechanism is reachable shall be documented
2719 • authentication factors shall be fabricated using specialized materials and tools as well as cumbersome
2720 extracted source materials. The duration of the fabrication process per authentication factor is not restricted.

2721 **Assessment activities:**

- 2722 • authentication at the created genuine enrolled biometric template shall be attempted using the correct genuine
2723 enrolled biometric template identifier, if present, and at least two fabricated authentication factors tried at least
2724 five times with slightly different parameters each

- 2725 • the outcome and used authentication factor of each attempt shall be recorded

2726 **Assignment of verdict:**

2727 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts.

2728 The verdict FAIL shall be assigned otherwise.

2729 **Supporting Evidence:**

- 2730 • description of the performed test
2731 • all test records of the performed test

2732 E.1.2.4 Assessment criteria regarding the protection against limited brute force
2733 attacks

2734 **Assessment objective:**

2735 The assessment covers functional testing of authentication mechanisms that provide a basic level of protection and use
2736 authentication factors of the type knowledge against limited brute force attacks.

2737 **Assessment preparation:**

- 2738 • the internet connected toy shall be set up in default configuration
- 2739 • at least one interface, where the authentication mechanism is reachable shall be documented

2740 the security insurance time (T_{SI}) for this assessment is 10 minutes (600s)

2741 **Assessment activities:**

2742 the minimal recommended complexity of passwords accepted by the mechanism ($C_{PW,min}$) shall be determined;
2743 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

2744 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
2745 per login attempt + a one-hour waiting period after 5 failed login attempts

2746 the probability of guessing a completely random password of the minimal recommended complexity (p_{GRP}) shall be
2747 calculated by $p_{GRP} = T_{SI} * f_{LA,max} / C_{PW,min}$

- 2748 • the methods and outcome of each step shall be recorded

2749 **Assignment of verdict:**

2750 The verdict PASS shall be assigned if the calculated probability p_{GRP} is less than 10^{-2} .

2751 The verdict FAIL shall be assigned otherwise.

2752 **Supporting Evidence:**

- 2753 • the authentication mechanism and the interface via which it was accessed
- 2754 • all test records of the performed test

2755 E.1.2.5 Assessment criteria regarding the protection against targeted brute force
2756 attacks

2757 **Assessment objective:**

2758 The assessment covers functional testing of authentication mechanisms that provide an enhanced level of protection and
2759 use authentication factors of the type knowledge against targeted brute force attacks.

2760 **Assessment preparation:**

- 2761 • the internet connected toy shall be set up in default configuration
- 2762 • at least one interface, where the authentication mechanism is reachable shall be documented

2763 the security insurance time (T_{SI}) for this assessment one month ($2,6 * 10^6s$)

2764 **Assessment activities:**

2765 the minimal recommended complexity of passwords accepted by the mechanism ($C_{PW,min}$) shall be determined; e.g.,
2766 $C_{PW,min} = (26 * 2 + 10)^8$ for minimum 8 characters of upper-case or lower-case letters or numbers

2767 the maximum sustained login attempt frequency ($f_{LA,max}$) shall be determined; e.g. $f_{LA,max} = (0,1s)^{-1}$ for 10 login
 2768 attempt per second

2769 the probability of guessing a completely random password of the minimal recommended complexity (p_{GRP}) shall be
 2770 calculated by $p_{GRP} = T_{SI} * f_{LA,max} / C_{PW,min}$

- 2771 • the methods and outcome of each step shall be recorded

2772 **Assignment of verdict:**

2773 The verdict PASS shall be assigned if the calculated probability p_{GRP} is less than 10^{-6} .

2774 The verdict FAIL shall be assigned otherwise.

2775 **Supporting Evidence:**

- 2776 • the authentication mechanism and the interface via which it was accessed
- 2777 • all test records of the performed test

2778 **E.1.2.6 Assessment criteria regarding the protection against automated brute force**
 2779 **attacks**

2780 **Assessment objective:**

2781 The assessment covers functional testing of authentication mechanisms that provide a medium level of protection and
 2782 use authentication factors of the type knowledge against targeted brute force attacks.

2783 **Assessment preparation:**

- 2784 • the internet connected toy shall be set up in default configuration
- 2785 • at least one interface, where the authentication mechanism is reachable shall be documented

2786 the security insurance time (T_{SI}) for this assessment is one day (86400s)

2787 **Assessment activities:**

2788 the minimal recommended complexity of passwords accepted by the mechanism ($C_{PW,min}$) shall be determined;
 2789 e.g. $C_{PW,min} = (26 * 2 + 10)^8$ for minimum 8 characters of upper-case case or lower-case letters or numbers

2790 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
 2791 per login attempt + a one-hour waiting period after 5 failed login attempts

2792 the probability of guessing a completely random password of the minimal recommended complexity (p_{GRP}) shall be
 2793 calculated by $p_{GRP} = T_{SI} * f_{LA,max} / C_{PW,min}$

- 2794 • the methods and outcome of each step shall be recorded

2795 **Assignment of verdict:**

2796 The verdict PASS shall be assigned if the calculated probability p_{GRP} is less than 10^{-6} .

2797 The verdict FAIL shall be assigned otherwise.

2798 **Supporting Evidence:**

- 2799 • the authentication mechanism and the interface via which it was accessed
- 2800 • all test records of the performed test

2801 **E.1.2.7 Assessment criteria regarding the protection against presentation attacks**

2802 **Assessment objective:**

2803 The assessment covers functional testing of authentication mechanisms that provide a medium level of protection and
 2804 use authentication factors of the type inherence against presentation attacks.

2805 **Assessment preparation:**

- 2806 • the internet connected toy shall be set up in default configuration
- 2807 • a genuine enrolled biometric template in the corresponding authentication mechanism with credential for
 2808 authentication shall be created
- 2809 • at least one interface, where the authentication mechanism is reachable shall be documented
- 2810 • authentication factors shall be fabricated using readily available materials and tools as well as readily available
 2811 source materials. The fabrication process shall not be longer than *twenty* minutes per authentication factor.

2812 NOTE: Readily available source materials are e.g. fingerprints on everyday items or publicly available photos.
 2813 Readily available materials and tools are of adhesive tape, printer paper, common printers.

2814 **Assessment activities:**

- 2815 • authentication at the created account shall be attempted using the correct account name, if present, and at least
 2816 two fabricated authentication factors tried at least five times with slightly different parameters each
- 2817 • the outcome and used fabricated authentication factor of each attempt shall be recorded

2818 **Assignment of verdict:**

2819 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts.

2820 The verdict FAIL shall be assigned otherwise.

2821 **Supporting Evidence:**

- 2822 • description of the performed test
- 2823 • all test records of the performed test

2824 **E.1.2.8 Assessment criteria regarding the protection against elaborate brute force**
 2825 **attacks**

2826 **Assessment objective:**

2827 The assessment covers functional testing of authentication mechanisms that provide a high level of protection and use
 2828 authentication factors of the type knowledge against targeted brute force attacks.

2829 **Assessment preparation:**

- 2830 • the internet connected toy shall be set up in default configuration
- 2831 • at least one interface, where the authentication mechanism is reachable shall be documented

2832 the security insurance time (T_{SI}) for this assessment is five years ($1,6 * 10^8 s$)

2833 **Assessment activities:**

2834 the minimal recommended complexity of passwords accepted by the mechanism ($C_{PW,min}$) shall be determined;
 2835 e.g. $(26 * 2 + 10)^8$ for minimum 8 characters of upper-case case or lower-case letters or numbers

2836 the maximum sustained login attempt frequency ($f_{LA,max}$) shall be determined; e.g. $(0,1s)^{-1}$ for 10 login attempt per
 2837 second

2838 the probability of guessing a completely random password of the minimal recommended complexity (p_{GRP}) shall be
 2839 calculated by $p_{GRP} = T_{SI} * f_{LA,max} / C_{PW,min}$

- 2840 • the methods and outcome of each step shall be recorded

2841 **Assignment of verdict:**

2842 The verdict PASS shall be assigned if the calculated probability is less than 10^{-6} .

2843 The verdict FAIL shall be assigned otherwise.

2844 **Supporting Evidence:**

2845 • the authentication mechanism and the interface via which it was accessed

2846 • all test records of the performed test

2847 **E.1.2.9 Assessment criteria regarding the protection against automated security**
2848 **token spoofing attacks**

2849 **Assessment objective:**

2850 The assessment covers functional testing of authentication mechanisms that provide a medium level of protection and
2851 use authentication factors of the type possession against automated security token spoofing attacks.

2852 **Assessment preparation:**

2853 • the internet connected toy shall be set up in default configuration

2854 • an account in the corresponding authentication mechanism with a security token for authentication shall be
2855 created

2856 • at least one interface, where the authentication mechanism is reachable shall be documented

2857 • security tokens, that match specifications of the interfaces, via which the authentication mechanism is
2858 reachable, shall be prepared or created without using any specific knowledge of the authentication mechanism

2859 **Assessment activities:**

2860 • authentication at the created account shall be attempted using the correct account name, if present, and the
2861 prepared or created security tokens

2862 • the outcome and used authentication factor of each attempt shall be recorded

2863 **Assignment of verdict:**

2864 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts, except where the used
2865 authentication factor exactly matches the configured one.

2866 The verdict FAIL shall be assigned otherwise.

2867 **Supporting Evidence:**

2868 • description of the performed test

2869 • all test records of the performed test

2870 **E.1.2.10 Assessment criteria regarding the protection against targeted security token**
2871 **spoofing attacks**

2872 **Assessment objective:**

2873 The assessment covers functional testing of authentication mechanisms that provide an enhanced level of protection and
2874 use authentication factors of the type possession against targeted security token spoofing attacks.

2875 **Assessment preparation:**

2876 • the internet connected toy shall be set up in default configuration

- 2877 • an account in the corresponding authentication mechanism with a security token for authentication shall be
2878 created
- 2879 • at least one interface, where the authentication mechanism is reachable shall be documented
- 2880 • security tokens, shall be prepared or created, which match the specifications of the authentication mechanism.

2881 **Assessment activities:**

- 2882 • authentication at the created account shall be attempted using the correct account name, if present, and the
2883 prepared or created security tokens
- 2884 • the outcome and used authentication factor of each attempt shall be recorded

2885 **Assignment of verdict:**

2886 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts, except where the used
2887 authentication factor exactly matches the configured one.

2888 The verdict FAIL shall be assigned otherwise.

2889 **Supporting Evidence:**

- 2890 • description of the performed test
- 2891 • all test records of the performed test

2892 **E.1.2.11 Assessment criteria regarding the protection against elaborate security token**
2893 **spoofing attacks**

2894 **Assessment objective:**

2895 The assessment covers functional testing of authentication mechanisms that provide a high level of protection and use
2896 authentication factors of the type possession against elaborate security token spoofing attacks.

2897 **Assessment preparation:**

- 2898 • the internet connected toy shall be set up in default configuration
- 2899 • an account in the corresponding authentication mechanism with a security token for authentication shall be
2900 created
- 2901 • at least one interface, where the authentication mechanism is reachable shall be documented
- 2902 • security tokens, shall be prepared or created, which match the specifications of the authentication mechanism
2903 and use information extracted from the original security token.

2904 **Assessment activities:**

- 2905 • authentication at the created account shall be attempted using the correct account name, if present, and the
2906 prepared or created security tokens
- 2907 • the outcome and used authentication factor of each attempt shall be recorded

2908 **Assignment of verdict:**

2909 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts, except where the used
2910 authentication factor exactly matches the configured one.

2911 The verdict FAIL shall be assigned otherwise.

2912 **Supporting Evidence:**

- 2913 • description of the performed test

- 2914
- all test records of the performed test

2915 E.1.2.12 Assessment criteria regarding the protection against replay attacks

2916 **Assessment objective:**

2917 The assessment covers functional testing of authentication mechanisms that use authentication factors of the type
2918 knowledge or possession (e.g. a session token) against replay attacks.

2919 **Assessment preparation:**

- 2920
- the internet connected toy shall be set up in default configuration
- 2921
- the authentication mechanism shall be active
- 2922
- a communication partner with active authentication mechanisms shall be set up for the internet connected toy
- 2923
- a capture and replay tool between internet connected toy and its communication partner shall be set up
- 2924
- at least one interface, where the authentication mechanism is reachable shall be documented

2925 **Assessment activities:**

- 2926
- Initiate a connection between the internet connected toy and its communication partner.
- 2927
- Use a capture tool to record the transmitted message or transaction data.
- 2928
- Replay (retransmit) the captured message to the product using a suitable tool in place to mimic the original
2929 communication partner.
- 2930
- Record if the product accepts the retransmitted data

2931 **Assignment of verdict:**

2932 The verdict PASS shall be assigned if it is not possible to impersonate as the communication partner.

2933 The verdict FAIL shall be assigned otherwise.

2934 **Supporting Evidence:**

- 2935
- description of the performed test
- 2936
- all test records of the performed test

2937 E.1.2.13 Assessment criteria regarding the protection against PitM attacks

2938 **Assessment objective:**

2939 The assessment covers functional testing of authentication mechanisms that use authentication factors of the type
2940 knowledge or possession (e.g. a session token) against PitM attacks.

2941 **Assessment preparation:**

- 2942
- the internet connected toy shall be set up in default configuration
- 2943
- the authentication mechanism shall be active
- 2944
- a communication partner with active authentication mechanisms shall be set up for the internet connected toy
- 2945
- a capture and PitM tool between internet connected toy and its communication partner shall be set up
- 2946
- at least one interface, where the authentication mechanism is reachable shall be documented

2947 **Assessment activities:**

- 2948
- Initiate a connection between the internet connected toy and its communication partner.

- 2949 • Attempt to capture data (user credentials, tokens, etc.) with the tool in place and actively intercept
2950 communication to impersonate the communication partner during:
- 2951 - generation and communication of authentication factors for the communication partner (if not
2952 pre-configured); and
- 2953 - authentication of the communication partner
- 2954 • Record if the impersonation as communication partner is successful

2955 **Assignment of verdict:**

2956 The verdict PASS shall be assigned if it is not possible to impersonate as the communication partner.

2957 The verdict FAIL shall be assigned otherwise.

2958 **Supporting Evidence:**

- 2959 • description of the performed test
- 2960 • all test records of the performed test

2961 **E.2 integrity protection strength**

2962 **E.2.1 [INT-SWPCK] Software package verification**

2963 **E.2.1.1 General**

2964 The present document specifies software package verification mechanisms' strength, by certain protection measures.
2965 Those measures are constructed such that measures of higher strength typically have less attack vectors than lower
2966 strength measures.

2967 **E.2.1.2 software package integrity verification - strength level basic**

2968 Mechanisms for the software package integrity verification - strength level basic shall:

- 2969 • explicitly obtain the confirmation of an authorized entity that the integrity and authenticity of a software
2970 package has been verified by the entity, where the software package's source is determined by the entity; or
- 2971 • explicitly obtain the confirmation of an authorized entity that the authenticity of a software package has been
2972 verified by the entity and use a hash or checksum provided by the entity for the software package to verify its
2973 integrity, where the software package's source is determined by the entity.

2974 **E.2.1.3 software package integrity verification - strength level normal**

2975 Mechanisms for the software package integrity verification - strength level normal shall ensure that a software package
2976 has been obtained from a trusted source over a secure communication channel that meets INT.COM.Enhanced.

2977 **E.2.1.4 software package integrity verification - strength level enhanced**

2978 Mechanisms for the software package integrity verification - strength level enhanced shall verify the authenticity and
2979 integrity of a software package using cryptographic digital signature verification.

2980 **E.2.2 [INT-COM] Communication of integrity relevant data**

2981 **E.2.2.1 General**

2982 The present document specifies the strength of mechanisms to protect the integrity of communicated integrity relevant
2983 data by their resistance against certain attack types. Those attack types are constructed such that mechanisms of higher
2984 strength protect against all attack types required for lower strengths.

2985 E.2.2.2 communication of integrity relevant data - protection strength level basic

2986 The communication of integrity relevant data - protection strength level basic shall protect against the following attack
2987 types:

2988 **accidental bit flip:** Accidental change of data by natural causes.

2989 E.2.2.3 communication of integrity relevant data - protection strength level normal

2990 The communication of integrity relevant data - protection strength level normal shall protect against the following
2991 attack types:

2992 **replay attack:** An attacker intercepts valid transmissions and then retransmits those captured messages to the same
2993 interface to deceive it into performing unauthorized actions.

2994 **accidental bit flip:** Accidental change of data by natural causes.

2995 **direct identity spoofing attack:** An attacker mimics another entity to gain a trust relationship with the internet
2996 connected toy

2997 **downgrade of communication protocols attack:** An attacker forces to use of a legacy, less secure, communication
2998 protocol

2999 E.2.2.4 communication of integrity relevant data - protection strength level enhanced

3000 The communication of integrity relevant data - protection strength level enhanced shall protect against the following
3001 attack types:

3002 **replay attack:** An attacker intercepts valid transmissions and then retransmits those captured messages to the same
3003 interface to deceive it into performing unauthorized actions.

3004 **person in the middle attack:** An attacker secretly alters the communication between the internet connected toy and
3005 another entity or another part of the internet connected toy to gain a trusted relationship with the involved
3006 communication partners without their knowledge.

3007 **accidental bit flip:** Accidental change of data by natural causes.

3008 **direct identity spoofing attack:** An attacker mimics another entity to gain a trust relationship with the internet
3009 connected toy

3010 **downgrade of communication protocols attack:** An attacker forces to use of a legacy, less secure, communication
3011 protocol

3012 E.2.2.5 communication of integrity relevant data - protection strength level strong

3013 The communication of integrity relevant data - protection strength level strong shall protect against the following attack
3014 types:

3015 **replay attack:** An attacker intercepts valid transmissions and then retransmits those captured messages to the same
3016 interface to deceive it into performing unauthorized actions.

3017 **person in the middle attack:** An attacker secretly alters the communication between the internet connected toy and
3018 another entity or another part of the internet connected toy to gain a trusted relationship with the involved
3019 communication partners without their knowledge.

3020 **accidental bit flip:** Accidental change of data by natural causes.

3021 **direct identity spoofing attack:** An attacker mimics another entity to gain a trust relationship with the internet
3022 connected toy

3023 **downgrade of communication protocols attack:** An attacker forces to use of a legacy, less secure, communication
3024 protocol

3025 **E.3 confidentiality protection strength**

3026 **E.3.1 [CONF-SSM] Confidentiality protecting persistent storage for**
3027 **confidential data**

3028 **E.3.1.1 General**

3029 The present document specifies confidentiality protecting secure storage mechanisms' strength, by certain security
3030 properties. Those properties are constructed such that mechanisms of higher strength have the properties of lower
3031 strength mechanisms.

3032 **E.3.1.2 confidential persistent storage - strength level basic**

3033 Mechanisms for the confidential persistent storage - strength level basic shall encrypt such that decryption is only
3034 possible for the internet connected toy.

3035 **E.3.1.3 confidential persistent storage - strength level normal**

3036 Mechanisms for the confidential persistent storage - strength level normal shall encrypt such that decryption is

- 3037 • only possible for the internet connected toy and
3038 • only performed after a successful authentication.

3039 **E.3.1.4 confidential persistent storage - strength level enhanced**

3040 Mechanisms for the confidential persistent storage - strength level enhanced shall encrypt supported by hardware, such
3041 that

- 3042 • decryption is only possible for the internet connected toy after a successful authentication and
3043 • the extraction of the encryption key is prevented by hardware.

3044 **E.3.1.5 confidential persistent storage - strength level strong**

3045 Mechanisms for the confidential persistent storage - strength level strong shall prevent the extraction of data by
3046 hardware.

3047 **E.3.2 [CONF-COM] Communication of confidential data**

3048 **E.3.2.1 General**

3049 The present document specifies the strength of mechanisms to protect the confidentiality of communicated confidential
3050 data by their resistance against certain attack types. Those attack types are constructed such that mechanisms of higher
3051 strength protect against all attack types required for lower strengths.

3052 **E.3.2.2 authentication - strength level strong**

3053 The authentication - strength level strong shall protect against the following attack types:

3054 **eavesdropping:** An attacker secretly intercepts the communication between the internet connected toy and another
3055 entity or another part of the internet connected toy.

3056 **E.3.2.3 communication of confidential data - protection strength level normal**

3057 The communication of confidential data - protection strength level normal shall protect against the following attack
3058 types:

3059 **eavesdropping:** An attacker secretly intercepts the communication between the internet connected toy and another
3060 entity or another part of the internet connected toy.

3061 **direct identity spoofing attack:** An attacker mimics another entity to gain a trust relationship with the internet
3062 connected toy

3063 **downgrade of communication protocols attack:** An attacker forces to use of a legacy, less secure, communication
3064 protocol

3065 E.3.2.4 communication of confidential data - protection strength level enhanced

3066 The communication of confidential data - protection strength level enhanced shall protect against the following attack
3067 types:

3068 **eavesdropping:** An attacker secretly intercepts the communication between the internet connected toy and another
3069 entity or another part of the internet connected toy.

3070 **person in the middle attack:** An attacker secretly alters the communication between the internet connected toy and
3071 another entity or another part of the internet connected toy to gain a trusted relationship with the involved
3072 communication partners without their knowledge.

3073 **direct identity spoofing attack:** An attacker mimics another entity to gain a trust relationship with the internet
3074 connected toy

3075 **downgrade of communication protocols attack:** An attacker forces to use of a legacy, less secure, communication
3076 protocol

3077 E.3.2.5 communication of confidential data - protection strength level strong

3078 The communication of confidential data - protection strength level strong shall protect against the following attack
3079 types:

3080 **eavesdropping:** An attacker secretly intercepts the communication between the internet connected toy and another
3081 entity or another part of the internet connected toy.

3082 **person in the middle attack:** An attacker secretly alters the communication between the internet connected toy and
3083 another entity or another part of the internet connected toy to gain a trusted relationship with the involved
3084 communication partners without their knowledge.

3085 **direct identity spoofing attack:** An attacker mimics another entity to gain a trust relationship with the internet
3086 connected toy

3087 **downgrade of communication protocols attack:** An attacker forces to use of a legacy, less secure, communication
3088 protocol

3089 Annex F (informative): Relationship between the present 3090 document and the covered/not covered cybersecurity risks

3091 **This informative annex is intended to provide the relevant information on the covered/not covered cybersecurity**
3092 **risks and still under discussion.**

3093 **The information provided in the column "Risk coverage" is based on a preliminary analysis which is planned to**
3094 **be expanded in the future and still under discussion.**

3095

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 internet connected toy		<p>Prevention: [ACM-FH] 5.1.3.1 [AUM-FH] 5.1.3.3 [AUTHZ-LP] 5.1.3.4 [AUTHZ-R] 5.1.3.5 [AUTHZ-PC] 5.1.3.6 [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 [PARCONT] 5.1.3.2 [SDC-AUM-FH] 5.1.2.1 [SDC-PARCONT] 5.1.2.5</p> <p>Information: [LOG-LOW] 5.1.10.1 [LOG-MEDIUM] 5.1.10.2 [LOG-HIGH] 5.1.10.3 [LOG-TIME] 5.1.10.4 [LOG-TIME-HIGH] 5.1.10.5 [LOG-STORAGE] 5.1.10.6 [LOG-BACKUP] 5.1.10.7 [USERNOT-NOSECFUC] 5.1.12.1</p> <p>Restoration: [SDC-FRM] 5.1.2.4</p>	COM, IF and POE	C
[2]	A threat actor	tamper s	integrity relevant data	permanently stored on the internet connected toy				N
[3]	A threat actor	tamper s	integrity relevant data	volatile stored on the internet connected toy				N
[4]	A threat actor	tamper s	integrity relevant data	communicated from or to the architectural component		<p>Prevention: [INT-COM] 5.1.4.2</p>	COM, IF and POE	C
[5]	A threat actor	discloses	confidential data	on the internet connected toy	unnecessarily processed	<p>Prevention: [DMIN-DJST] 5.1.6.1</p>		C
[6]	A threat actor	discloses	confidential data	permanently stored on the internet connected toy	during storage	<p>Prevention: [CONF-SSM] 5.1.5.1</p>	POE	C
[7]	A threat actor	discloses	confidential data	permanently stored on the internet connected toy	after deletion	<p>Prevention: [DLM-PERM] 5.1.11.1</p>		N
[8]	A threat actor	discloses	confidential data	volatile stored on the internet connected toy	during usage			N
[9]	A threat actor	discloses	confidential data	volatile stored on the internet connected toy	after usage			N
[10]	A threat actor	discloses	confidential data	communicated from or to the architectural component		<p>Prevention: [CONF-COM] 5.1.5.2</p>	COM, IF and POE	C
[11]	A threat actor	tamper s	loss sensitive data	permanently stored on the internet connected toy	during storage			N

No.	Threat Actor	Threat action	Asset	Threat details		Requirement(s) for mitigation	Relevant attack surface parameter	Risk coverage
[12]	A threat actor	tamper s	integrity relevant function	on the internet connected toy		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 internet connected toy	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 internet connected toy	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 internet connected toy	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 internet connected toy	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 internet connected toy		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 internet connected toy	because the user is not aware of security relevant information	Prevention: [USERNOT-SECRET] 5.1.12.2 Information: [USERNOT-SECRET] 5.1.12.2	IF.Human	C
[20]	A user	unknowingly creates confidential	audio or video capture data	on the internet connected toy			IF.Human	C

- 3096
- 3097
- The columns *Threat Actor*, *Threat Action*, *Asset*, and *Threat Details* describe the threat scenario under consideration.
- 3098
- 3099
- The column *Requirement(s) for mitigation* refers to the mitigations of the risks that arise from the threat scenario.
- 3100
- 3101
- The *Relevant attack surface parameter* column describes which of the attack surface parameters make a difference in mitigation.
- 3102
- 3103
- 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).

3104

Annex G (informative): Relationship between the present document and ETSI EN 303 645/ ETSI TS 103 701

3105

3106

This informative annex is intended to provide a mapping between the present document and the content of ETSI TC CYBER's existing work on CIoT devices (ETSI EN 303 645/ ETSI TS 103 701).

3107