



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

Reference

DEN/CYBER-EUS-004

Keywords

CRA, cybersecurity

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the
[ETSI Search & Browse Standards](#) application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed,
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part of this document may be reproduced in any form, by any means and in any media, without the prior written authorization of ETSI and except as expressly permitted below.

By way of exception and when the document is a normative deliverable (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)), ETSI authorizes to reproduce and incorporate into products, services and technical documentation only those extracts (e.g. templates) that are strictly necessary for the technical implementation of the normative deliverable, to ensure compliance with the latter. Nothing in this notice shall be construed as limiting any mandatory exceptions to copyright provided by applicable law.

© ETSI 2026.
All rights reserved.

Contents

Intellectual Property Rights	10
Foreword.....	10
Modal verbs terminology	11
Introduction	11
1 Scope	12
2 References	12
2.1 Normative references	12
2.2 Informative references	12
3 Definition of terms, symbols and abbreviations.....	13
3.1 Terms	13
3.1.1 Architecture related terms	13
3.1.2 Asset categories.....	14
3.1.3 Communication types.....	14
3.1.4 Data assets.....	15
3.1.5 Data related terms	16
3.1.6 Function assets	17
3.1.7 Function related terms.....	18
3.1.8 Interface	22
3.1.9 Operational environments	22
3.1.10 Users.....	23
3.2 Symbols	23
3.3 Abbreviations.....	24
4 Product context.....	26
4.1 Product functions	26
4.1.1 Function assets	26
4.1.2 Data assets.....	26
4.2 Product architecture	27
4.3 Operational environment	28
4.3.1 General description	28
4.3.2 Physical/Hardware environment	28
4.3.3 Logical/Software environment	28
4.3.4 Connectivity aspects.....	28
4.4 Distribution of security functions	29
4.5 Users	29
4.6 Use cases.....	29
5 Technical requirements for products	29
5.1 Introduction - Applicability of the requirements	29
5.2 Appropriate level of cybersecurity.....	30
5.2.0 Introduction on appropriate level of cybersecurity requirements	30
5.2.1 [USERNOT-NOSECFUC] User notifications on not available security functions.....	30
5.2.2 [USERNOT-SECREL] Language and representation for security-related user notifications	30
5.2.3 [GUI-SECONF] Visual representation of security-related configuration via GUIs	30
5.2.4 [BACKUP-TRANS] Data transfer mechanisms for loss sensitive data	30
5.2.5 [BACKUP-AUTOTRANS] Automatic data transfer mechanisms for loss sensitive data	30
5.2.6 [BACKUP-EXPORT] Data export mechanisms for loss sensitive data.....	30
5.3 No known exploitable vulnerabilities	31
5.3.0 Introduction on no known exploitable vulnerabilities	31
5.3.1 [NKEV-MKAV] No known exploitable vulnerabilities	31
5.3.2 [NKEV-INIT-UDP] Initial security update before or during first use	31
5.4 Secure by default configuration	31
5.4.0 Introduction on secure by default configuration.....	31
5.4.1 [SDC-AUM-FH] Default configuration of authentication for functions whose use can cause harm	31
5.4.2 [SDC-SUM-AUTO] Default configuration of automated security updates	32

5.4.3	[SDC-SUM-NOTIF] Default configuration of update notifications	32
5.4.4	[SDC-FRM] Factory reset to restore the default state	32
5.4.5	[SDC-PARCONT] Default configuration for parental control	32
5.4.6	[SDC-MON-HANDLE] Handling of events by default	33
5.4.7	[CRY-GENERAL] General requirements related to cryptography	33
5.4.8	[CRY-CCK-PRE-LEN] Key size of preinstalled long term confidential cryptographic keys	33
5.4.9	[CRY-CCK-GEN] Default key size of generated long term confidential cryptographic keys	33
5.4.10	[CRY-PW-PRE-COM] Complexity of preinstalled passwords	33
5.4.11	[CRY-PW-GEN-COM] Default complexity of generated passwords	33
5.4.12	[CRY-PW-USR-COM] Recommended complexity of user chosen passwords	34
5.5	Security updates	34
5.5.0	Introduction on security updates	34
5.5.1	[SU-SUPPORT] Secure software update mechanism	34
5.5.2	[SU-PROVIDE] Secure software update mechanism for core components	34
5.5.3	[SU-AUTO] Automated security updates	34
5.5.4	[SU-DISABLE-AUTO] Option to disable automated security updates	35
5.5.5	[SU-POSTPONE-AUTO] Option to postpone automated security updates	35
5.5.6	[SU-NOTIF] Update notifications	35
5.6	Authentication and access control	35
5.6.0	Introduction on authentication and access control	35
5.6.1	[ACM-FH] Access control for functions whose use can cause harm	35
5.6.2	[PARCONT] Support of parental control	36
5.6.3	[AUM-FH] Authentication for functions whose use can cause harm	36
5.6.4	[AUTHZ-LP] Least privilege in authorisation policies	37
5.6.5	[AUTHZ-R] Revocability of granted permissions	37
5.6.6	[AUTHZ-PC] Authorisation policies for parental control	37
5.7	Confidentiality protection	37
5.7.0	Introduction on confidentiality protection	37
5.7.1	[CONF-SSM] Confidentiality protecting persistent storage for confidential data	38
5.7.2	[CONF-COM] Communication of confidential data	38
5.8	Integrity protection	39
5.8.0	Introduction on integrity protection	39
5.8.1	[INT-SSM] Integrity protecting persistent storage for integrity relevant data	39
5.8.2	[INT-COM] Communication of integrity relevant data	39
5.8.3	[INT-SWPCK] Software package verification	40
5.9	Data minimisation	40
5.9.0	Introduction on data minimisation	40
5.9.1	[DMIN-DJST] Minimise processed data	40
5.10	Availability protection	41
5.10.0	Introduction on availability protection	41
5.10.1	[AVAI-TIME-RECO-POW] Restoration after loss of power	41
5.10.2	[AVAI-TIME-NETW] Local operation	41
5.10.3	[AVAI-TIME-RECO-NETW] Restoration after loss of network connection	41
5.10.4	[AVAI-TIME-OUTA-NOT] Notify non-availability	41
5.10.5	[AVAI-TIME-PREV-NOT] Notify upcoming limitation	41
5.10.6	[AVAI-TIME-NET-PRIO] Network prioritisation	42
5.10.7	[AVAI-TIME-RES-PRIO] Power resource prioritisation	42
5.10.8	[AVAI-TIME-DOS-RATE] Incoming rate limiting	42
5.10.9	[AVAI-SUM-SCHEDULE] Scheduling of updates	42
5.11	Non-interference	42
5.11.0	Introduction on non-interference	42
5.11.1	[NOINF-AMP] Amplification control	42
5.12	Attack surface minimisation	43
5.12.0	Introduction on attack surface minimisation	43
5.12.1	[LAS-INVAL] Validation of external data input	43
5.12.2	[LAS-INSAN] Sanitisation of external data input	43
5.12.3	[LAS-PHY-INF] Only necessary physical interfaces	43
5.12.4	[LAS-LOGIC-INF] Only necessary logical interfaces active by default	43
5.12.5	[LAS-APP] Only necessary apps by default	43
5.12.6	[LAS-SBOOT] Secure boot	43
5.13	Exploit mitigation	44
5.13.0	Introduction on exploit mitigation	44

5.13.1	[PRIV-DATA-HIGH] Privileged access on impact class high data assets	44
5.13.2	[PRIV-FUNC-HIGH] Privileged access on impact class high function assets	44
5.14	Monitoring.....	44
5.14.0	Introduction on monitoring	44
5.14.1	[MON-LOW] Events to log for low risk internet connected toy.....	44
5.14.2	[MON-MEDIUM] Events to log for medium risk internet connected toy	45
5.14.3	[MON-HIGH] Events to log for high risk internet connected toy.....	45
5.14.4	[MON-HANDLE] Handling of events.....	45
5.14.5	[LOG-TIME] Timestamps for logs	45
5.14.6	[LOG-TIME-HIGH] Real-time timestamps for logs.....	46
5.14.7	[LOG-STORE-MEDIUM] Logfile persistence for medium risk internet connected toy	46
5.14.8	[LOG-STORE-HIGH] Logfile persistence for high risk internet connected toy	46
5.14.9	[LOG-CONFIG] Configuration of logging mechanisms	46
5.15	Factory reset and data portability	46
5.15.0	Introduction on factory reset and data portability	46
5.15.1	[DLM-PERM] Permanent removal of user-related data	47
6	Assessment criteria for compliance with technical requirements	47
6.1	General.....	47
6.2	Appropriate level of cybersecurity.....	49
6.2.1	Assessment criteria for [USERNOT-NOSECFUC]	49
6.2.2	Assessment criteria for [USERNOT-SECREL]	49
6.2.3	Assessment criteria for [GUI-SECCONF]	50
6.2.4	Assessment criteria for [BACKUP-TRANS]	51
6.2.5	Assessment criteria for [BACKUP-AUTOTRANS]	53
6.2.6	Assessment criteria for [BACKUP-EXPORT]	54
6.3	No known exploitable vulnerabilities	55
6.3.1	Assessment criteria for [NKEV-MKAV]	55
6.3.2	Assessment criteria for [NKEV-INIT-UDP]	56
6.4	Secure by default configuration	58
6.4.1	Assessment criteria for [SDC-AUM-FH]	58
6.4.2	Assessment criteria for [SDC-SUM-AUTO]	59
6.4.3	Assessment criteria for [SDC-SUM-NOTIF]	60
6.4.4	Assessment criteria for [SDC-FRM]	61
6.4.5	Assessment criteria for [SDC-PARCONT]	62
6.4.6	Assessment criteria for [SDC-MON-HANDLE]	63
6.4.7	Assessment criteria for [CRY-GENERAL]	64
6.4.8	Assessment criteria for [CRY-CCK-PRE-LEN]	65
6.4.9	Assessment criteria for [CRY-CCK-GEN]	65
6.4.10	Assessment criteria for [CRY-PW-PRE-COM]	66
6.4.11	Assessment criteria for [CRY-PW-GEN-COM]	67
6.4.12	Assessment criteria for [CRY-PW-USR-COM]	68
6.5	Security updates.....	70
6.5.1	Assessment criteria for [SU-SUPPORT]	70
6.5.2	Assessment criteria for [SU-PROVIDE]	71
6.5.3	Assessment criteria for [SU-AUTO]	72
6.5.4	Assessment criteria for [SU-DISABLE-AUTO]	73
6.5.5	Assessment criteria for [SU-POSTPONE-AUTO]	74
6.5.6	Assessment criteria for [SU-NOTIF]	75
6.6	Authentication and access control	76
6.6.1	Assessment criteria for [ACM-FH]	76
6.6.2	Assessment criteria for [PARCONT]	78
6.6.3	Assessment criteria for [AUM-FH]	79
6.6.4	Assessment criteria for [AUTHZ-LP]	80
6.6.5	Assessment criteria for [AUTHZ-R]	81
6.6.6	Assessment criteria for [AUTHZ-PC]	82
6.7	Confidentiality protection	82
6.7.1	Assessment criteria for [CONF-SSM]	82
6.7.2	Assessment criteria for [CONF-COM]	84
6.8	Integrity protection	85
6.8.1	Assessment criteria for [INT-SSM]	85
6.8.2	Assessment criteria for [INT-COM]	87

6.8.3	Assessment criteria for [INT-SWPCK].....	88
6.9	Data minimisation.....	89
6.9.1	Assessment criteria for [DMIN-DJUST]	89
6.10	Availability protection	90
6.10.1	Assessment criteria for [AVAI-TIME-RECO-POW]	90
6.10.2	Assessment criteria for [AVAI-TIME-NETW].....	92
6.10.3	Assessment criteria for [AVAI-TIME-RECO-NETW].....	93
6.10.4	Assessment criteria for [AVAI-TIME-OUTA-NOT].....	95
6.10.5	Assessment criteria for [AVAI-TIME-PREV-NOT]	96
6.10.6	Assessment criteria for [AVAI-TIME-NET-PRIO]	98
6.10.7	Assessment criteria for [AVAI-TIME-RES-PRIO]	99
6.10.8	Assessment criteria for [AVAI-TIME-DOS-RATE]	100
6.10.9	Assessment criteria for [AVAI-SUM-SCHEDULE]	101
6.11	Non-interference	102
6.11.1	Assessment criteria for [NOINF-AMP]	102
6.12	Attack surface minimisation	103
6.12.1	Assessment criteria for [LAS-INVAL]	103
6.12.2	Assessment criteria for [LAS-INSAN]	105
6.12.3	Assessment criteria for [LAS-PHY-INF].....	106
6.12.4	Assessment criteria for [LAS-LOGIC-INF].....	106
6.12.5	Assessment criteria for [LAS-APP]	107
6.12.6	Assessment criteria for [LAS-SBOOT].....	108
6.13	Exploit mitigation	109
6.13.1	Assessment criteria for [PRIV-DATA-HIGH].....	109
6.13.2	Assessment criteria for [PRIV-FUNC-HIGH]	111
6.14	Monitoring.....	112
6.14.1	Assessment criteria for [MON-LOW].....	112
6.14.2	Assessment criteria for [MON-MEDIUM]	113
6.14.3	Assessment criteria for [MON-HIGH]	113
6.14.4	Assessment criteria for [MON-HANDLE]	114
6.14.5	Assessment criteria for [LOG-TIME]	116
6.14.6	Assessment criteria for [LOG-TIME-HIGH]	117
6.14.7	Assessment criteria for [LOG-STORE-MEDIUM]	118
6.14.8	Assessment criteria for [LOG-STORE-HIGH]	119
6.14.9	Assessment criteria for [LOG-CONFIG]	120
6.15	Factory reset and data portability.....	121
6.15.1	Assessment criteria for [DLM-PERM]	121

Annex A (informative):	Relationship between the present document and the essential cybersecurity requirements of EU Regulation (EU) 2024/2847.....	124
-------------------------------	--	------------

Annex B (informative):	Security analysis.....	128
-------------------------------	-------------------------------	------------

B.1	General	128
B.2	Assets	128
B.3	Risk factors.....	128
B.4	Assumptions	128
B.5	Threats.....	129
B.6	Relationship between the present document and the covered/not covered cybersecurity risks	129
B.7	Guidance for determining impact classes.....	132
B.7.1	General.....	132
B.7.2	Confidential data.....	132
B.7.3	Loss sensitive data	133
B.7.4	Time sensitive function.....	133
B.7.5	Integrity relevant data and integrity relevant function	134

Annex C:	Void	135
-----------------	-------------------	------------

Annex D (normative):	Relationship between specific data and functions assets covered by the present document to impact classes for generic asset categories	136
D.1	Data assets	136
D.2	Function assets	137
Annex E (normative):	Protection measures.....	139
E.1	Authentication mechanism strength	139
E.1.1	[AUM-FH] Authentication for functions whose use can cause harm	139
E.1.1.1	General	139
E.1.1.2	[AUM-E-I-Basic] AUTH.Basic inheritance based SFA	139
E.1.1.3	[AUM-E-K-Basic] AUTH.Basic knowledge based SFA	139
E.1.1.4	[AUM-E-I-Normal] AUTH.Normal inheritance based SFA	139
E.1.1.5	[AUM-E-K-Normal] AUTH.Normal knowledge based SFA	139
E.1.1.6	[AUM-E-P-Normal] AUTH.Normal possession based SFA	139
E.1.1.7	[AUM-E-MFA-Normal] AUTH.Normal MFA	140
E.1.1.8	[AUM-E-I-Enhanced] AUTH.Enhanced inheritance based SFA	140
E.1.1.9	[AUM-E-K-Enhanced] AUTH.Enhanced knowledge based SFA	140
E.1.1.10	[AUM-E-P-Enhanced] AUTH.Enhanced possession based SFA	140
E.1.1.11	[AUM-E-MFA-Enhanced] AUTH.Enhanced MFA	140
E.1.1.12	[AUM-E-I-Strong] AUTH.Strong inheritance based SFA	141
E.1.1.13	[AUM-E-P-Strong] AUTH.Strong possession based SFA	141
E.1.1.14	[AUM-E-MFA-Strong] AUTH.Strong MFA	141
E.1.1.15	[AUM-E-Replay] AUTH.Normal, AUTH.Enhanced and AUTH.Strong replay protection	141
E.1.1.16	[AUM-E-PitM] AUTH.Normal, AUTH.Enhanced and AUTH.Strong person in the middle protection	142
E.1.2	Assessment for [AUM-FH] authentication mechanism strength	142
E.1.2.1	General	142
E.1.2.2	Assessment criteria for [AUM-E-I-Basic]	142
E.1.2.3	Assessment criteria for [AUM-E-K-Basic]	143
E.1.2.4	Assessment criteria for [AUM-E-I-Normal]	144
E.1.2.5	Assessment criteria for [AUM-E-K-Normal]	145
E.1.2.6	Assessment criteria for [AUM-E-P-Normal]	145
E.1.2.7	Assessment criteria for [AUM-E-MFA-Normal]	147
E.1.2.8	Assessment criteria for [AUM-E-I-Enhanced]	148
E.1.2.9	Assessment criteria for [AUM-E-K-Enhanced]	149
E.1.2.10	Assessment criteria for [AUM-E-P-Enhanced]	150
E.1.2.11	Assessment criteria for [AUM-E-MFA-Enhanced]	152
E.1.2.12	Assessment criteria for [AUM-E-I-Strong]	153
E.1.2.13	Assessment criteria for [AUM-E-P-Strong]	154
E.1.2.14	Assessment criteria for [AUM-E-MFA-Strong]	155
E.1.2.15	Assessment criteria for [AUM-E-Replay]	156
E.1.2.16	Assessment criteria for [AUM-E-PitM]	157
E.2	Integrity protection strength	158
E.2.1	[INT-SSM] Integrity protecting persistent storage for integrity relevant data	158
E.2.1.1	General	158
E.2.1.2	[INT-SSM-E-Basic] INT.SSM.Basic integrity protecting secure storage mechanism	158
E.2.1.3	[INT-SSM-E-Normal] INT.SSM.Normal integrity protecting secure storage mechanism	159
E.2.1.4	[INT-SSM-E-Enhanced] INT.SSM.Enhanced integrity protecting secure storage mechanism	159
E.2.1.5	[INT-SSM-E-Strong] INT.SSM.Strong integrity protecting secure storage mechanism	159
E.2.2	Assessment for integrity protecting secure storage mechanism strength	159
E.2.2.1	General	159
E.2.2.2	Assessment criteria for [INT-SSM-E-Basic]	159
E.2.2.3	Assessment criteria for [INT-SSM-E-Normal]	160
E.2.2.4	Assessment criteria for [INT-SSM-E-Enhanced]	161
E.2.2.5	Assessment criteria for [INT-SSM-E-Strong]	162
E.2.3	[INT-COM] Communication of integrity relevant data	163
E.2.3.1	General	163
E.2.3.2	[INT-COM-E-Basic] INT.COM.Basic integrity protecting communication mechanism	163
E.2.3.3	[INT-COM-E-Normal] INT.COM.Normal integrity protecting communication mechanism	163

E.2.3.4	[INT-COM-E-Enhanced] INT.COM.Enhanced integrity protecting communication mechanism	163
E.2.3.5	[INT-COM-E-EndAuth] INT.COM.Normal and INT.COM.Enhanced integrity protecting communication mechanism endpoint authentication	164
E.2.3.6	[INT-COM-E-Downgrade] INT.COM.Normal and INT.COM.Enhanced integrity protecting communication mechanism downgrade protection	164
E.2.4	Assessment for integrity protecting communication mechanism strength	164
E.2.4.1	General	164
E.2.4.2	Assessment criteria for [INT-COM-E-Basic]	164
E.2.4.3	Assessment criteria for [INT-COM-E-Normal]	165
E.2.4.4	Assessment criteria for [INT-COM-E-Enhanced]	166
E.2.4.5	Assessment criteria for [INT-COM-E-EndAuth]	167
E.2.4.6	Assessment criteria for [INT-COM-E-Downgrade]	168
E.2.5	[INT-SWPCK] Software package verification	169
E.2.5.1	General	169
E.2.5.2	[INT-SWPCK-E-Basic] INT.SW.VER.Basic software package verification mechanism	169
E.2.5.3	[INT-SWPCK-E-Normal] INT.SW.VER.Normal software package verification mechanism	169
E.2.5.4	[INT-SWPCK-E-Enhanced] INT.SW.VER.Enhanced software package verification mechanism	170
E.2.6	Assessment for integrity protecting communication mechanism strength	170
E.2.6.1	General	170
E.2.6.2	Assessment criteria for [INT-SWPCK-E-Basic]	170
E.2.6.3	Assessment criteria for [INT-SWPCK-E-Normal]	171
E.2.6.4	Assessment criteria for [INT-SWPCK-E-Enhanced]	172
E.3	Confidentiality protection strength	173
E.3.1	[CONF-SSM] Confidentiality protecting persistent storage for confidential data	173
E.3.1.1	General	173
E.3.1.2	[CONF-SSM-E-Basic] CONF.SSM.Basic confidentiality protecting secure storage mechanism	173
E.3.1.3	[CONF-SSM-E-Normal] CONF.SSM.Normal confidentiality protecting secure storage mechanism	173
E.3.1.4	[CONF-SSM-E-Enhanced] CONF.SSM.Enhanced confidentiality protecting secure storage mechanism	174
E.3.1.5	[CONF-SSM-E-Strong] CONF.SSM.Strong confidentiality protecting secure storage mechanism	174
E.3.2	Assessment for integrity protecting secure storage mechanism strength	174
E.3.2.1	General	174
E.3.2.2	Assessment criteria for [CONF-SSM-E-Basic]	174
E.3.2.3	Assessment criteria for [CONF-SSM-E-Normal]	175
E.3.2.4	Assessment criteria for [CONF-SSM-E-Enhanced]	176
E.3.2.5	Assessment criteria for [CONF-SSM-E-Strong]	177
E.3.3	[CONF-COM] Communication of confidential data	178
E.3.3.1	General	178
E.3.3.2	[CONF-COM-E-Basic] CONF.COM.Basic confidentiality protecting communication mechanism	178
E.3.3.3	[CONF-COM-E-Normal] CONF.COM.Normal confidentiality protecting communication mechanism	178
E.3.3.4	[CONF-COM-E-Enhanced] CONF.COM.Enhanced confidentiality protecting communication mechanism	178
E.3.3.5	[CONF-COM-E-EndAuth] CONF.COM.Normal and CONF.COM.Enhanced confidentiality protecting communication mechanism endpoint authentication	179
E.3.3.6	[CONF-COM-E-Downgrade] CONF.COM.Normal and CONF.COM.Enhanced confidentiality protecting communication mechanism downgrade protection	179
E.3.4	Assessment for confidentiality protecting communication mechanism strength	179
E.3.4.1	General	179
E.3.4.2	Assessment criteria for [CONF-COM-E-Basic]	179
E.3.4.3	Assessment criteria for [CONF-COM-E-Normal]	180
E.3.4.4	Assessment criteria for [CONF-COM-E-Enhanced]	181
E.3.4.5	Assessment criteria for [CONF-COM-E-EndAuth]	182
E.3.4.6	Assessment criteria for [CONF-COM-E-Downgrade]	183
Annex F (informative):	Guidance for the application of the present document	185
Annexes G to J:	Void.....	188
Annex K (normative):	Generic cryptographic requirements and assessment.....	189
K.1	Cryptography.....	189

K.1.1	[CRY-SOTA] Requirement	189
K.1.2	Assessment criteria	190
K.1.2.1	Assessment criteria for [CRY-SOTA] concerning ACM-listed cryptographic mechanisms	190
K.1.2.2	Assessment criteria for [CRY-SOTA] concerning ACM-extended cryptographic mechanisms.....	191
K.1.2.3	Assessment criteria for [CRY-SOTA] concerning interoperability-based cryptographic mechanisms ...	192
K.2	Crypto agility	193
K.2.1	[CRY-AGIL] Requirement	193
K.2.2	Assessment criteria for [CRY-AGIL]	194
K.3	ACM-extended cryptographic mechanisms	195
K.3.1	[CRY-ACM-EXT] Requirement	195
K.3.2	List of ACM-extended cryptographic mechanisms	196
K.3.3	Assessment	196
K.4	Interoperability-based cryptographic mechanisms.....	196
K.4.1	[CRY-INTOP] Requirement	196
K.4.2	List of interoperability-based cryptographic mechanisms	197
K.4.3	Assessment	197
Annexes L to Q:	Void	198
Annex R (informative):	Guidance on RDPS	199
History		200

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

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

Foreword

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

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

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

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

Modal verbs terminology

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).

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

Introduction

The present document provides the technical cybersecurity requirements for the products in scope, following a risk-based approach in support of the Regulation (EU) 2024/2847 [i.1]. The technical cybersecurity requirements are thereby proportionate to the intended purpose, reasonably foreseeable use, deployment context, and threat exposure of the products.

- Clause [4](#) does not contain technical requirements; it describes the product context that is considered for the application of the present document.
- Clause [5](#) specifies technical cybersecurity requirements for the product to mitigate the identified risks, including their applicability conditions.
- Clause [6](#) specifies the assessment criteria and compliance verification procedures with the requirements of clause [5](#).
- Annex [A](#) maps the technical requirements of the present document with the essential requirements of the Regulation (EU) 2024/2847 [i.1].
- Annex [B](#) informs about the methodology used to assess the security risks of the products in their context.
- Annex [D](#) maps the data assets and function assets addressed by the present document to their impact classes. This mapping is necessary to identify the technical requirements and the related details that are to be applied for a product.
- Annex [E](#) provides specific technical requirements and related assessment criteria for certain protection measures that might be required for a product according to clause [5](#).
- Annex [F](#) provides guidance on the application of the present document.
- Annex [K](#) supports the definition of the cryptographic requirements and assessment criteria used by the present document.
- Annex [R](#) provides guidance on applying the technical requirements of the present document on remote data processing solutions (RDPS).

1 Scope

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

- are specified within the "technical description" of the "category of product" number "18." by the Commission Implementing Regulation (EU) 2025/2392 [i.2] as:
"Internet connected toys that have social interactive features are products with digital elements that are covered by Directive 2009/48/EC, that communicate on the public Internet, whether directly or via any other equipment, and that have embedded technologies that enable inbound and outbound communication, such as keyboard, microphone, speaker or camera." or "Internet connected toys that have location tracking features are products with digital elements that are covered by Directive 2009/48/EC, that communicate on the public Internet, whether directly or via any other equipment, and that have technologies that enable tracking or inferring of the geographical location of the toy or its user. Where the toy merely detects the proximity of the user or of other toys by using sensing technologies, the toy is not to be considered to have location tracking features." and
- are only covered within the product context described in clause 4.

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

2 References

2.1 Normative references

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

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

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

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

- [1] [Agreed Cryptographic Mechanisms](#); ENISA Report 1747792503 (version 2 - April 2025): "European Cybersecurity Certification Group Sub-group on Cryptography Agreed Cryptographic Mechanisms".

2.2 Informative references

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

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

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

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

- [i.2] [Commission Implementing Regulation \(EU\) 2025/2392](#) of 28 November 2025 on the technical description of the categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of the Council.
 - [i.3] [Standardisation request M/606 - C\(2025\)618](#): "Commission Implementing decision of 3.2.2025 on a standardisation request to the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)".
 - [i.4] prEN 40000-1-1: "Cybersecurity requirements for products with digital elements – Vocabulary" (produced by CEN CENELEC).
- NOTE: Version and date to be added upon its publication by CEN CENELEC.
- [i.5] prEN 40000-1-3: "Cybersecurity requirements for products with digital elements – Part 1-3: Vulnerability handling" (produced by CEN CENELEC).
- NOTE: Version and date to be added upon its publication by CEN CENELEC.
- [i.6] ETSI EN 304 623 (V1.1.1): "Cyber Security (CYBER); CRA; Cybersecurity requirements for boot managers".
 - [i.7] [ISO/IEC 24760-1:2025](#): "Information security, cybersecurity and privacy protection — A framework for identity management - Part 1: Core concepts and terminology".
 - [i.8] [ETSI TS 103 732-2 \(V1.1.1\)](#): "CYBER; Consumer Mobile Device; Part 2: Biometric Authentication Protection Profile Module".
 - [i.9] [NIST SP 800-78-5](#): "NIST; Cryptographic Algorithms and Key Sizes for Personal Identity Verification".
 - [i.10] [IETF RFC 8446](#): "The Transport Layer Security (TLS) Protocol Version 1.3".
 - [i.11] [IETF RFC 8613](#): "Object Security for Constrained RESTful Environments (OSCORE)".
 - [i.12] [IETF RFC 9528](#): "Ephemeral Diffie-Hellman Over COSE (EDHOC)".
 - [i.13] [IETF RFC 9147](#): "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3".
 - [i.14] [NIST FIPS 203](#): "Module-Lattice-Based Key-Encapsulation Mechanism Standard".
 - [i.15] [NIST FIPS 204](#): "Module-Lattice-Based Digital Signature Standard".
 - [i.16] [NIST SP 800-57-1](#): "Recommendation for Key Management: Part 1 - General".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

3.1.1 Architecture related terms

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

EXAMPLE: A mobile app, desktop software or parts of architectural component's embedded software that implements essential functionalities.

NOTE: Application software typically uses APIs provided by core software.

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

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

EXAMPLE: A hardware architectural component's operating system, hardware abstraction layer or APIs for application software.

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

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

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

3.1.2 Asset categories

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

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

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

function whose use can cause harm:

- function whose use can impact the availability of other devices, services or networks,
- function whose use can impact the safety or privacy of human entities,
- function which can communicate confidential data,
- function which can communicate integrity relevant data,
- function which can modify integrity relevant data, or
- function which can modify integrity relevant functions

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

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

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

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

3.1.3 Communication types

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

EXAMPLE: Communication through a virtual-private-network tunnel with a communication partner in a private network.

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

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

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

EXAMPLE: Communication via internet.

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

EXAMPLE: Communication with a hardware architectural component via its key-pad.

3.1.4 Data assets

activity data: data asset that describes physical movements, behaviours or activity patterns to monitor the personal fitness level of humans

audit event data: data asset that contains information produced by monitoring mechanisms that can be used by logging mechanisms

NOTE 1: Typically contains records of events relevant for the cybersecurity of the internet connected toy, its connected networks and other devices.

NOTE 2: Audit event data are typically user-related data.

authorisation policy data: data asset that contains an authorisation policy

EXAMPLE: Assignment of privileges to users.

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

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

device identifier data: data asset the identifies a specific device

entity's location data: data asset that is not public data and represents the location/position of an entity

NOTE: Entity including but not limited to user and architectural component.

function binary data: data asset stored on the internet connected toy that implements the logic of a internet connected toy's function asset.

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

identity data for authentication: data asset that contains identity information and that is not a cryptographic security parameter and used for authentication

EXAMPLE: Data containing user/device identifier.

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

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

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

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

private audio data: data asset that is not public data and represents audio information

EXAMPLE 1: Audio data recorded by the internet connected toy.

EXAMPLE 2: Audio data provided by the user.

NOTE: Private audio data does not include publicly accessible audio recordings from the internet.

private video data: data asset that is not public data and represents video information

EXAMPLE 1: Video or picture recordings processed (including storage) by the internet connected toy.

EXAMPLE 2: Video data provided by the user.

NOTE: Private video data does not include publicly accessible videos from the internet.

public data asset: data asset derived from public data

real-time data: data asset which represents (current) time and date

NOTE: Typically used for security specific processing, logging and communication (e.g. secure time validation such as certificate date validation, time of an intrusion/hold-up event, time synchronisation).

social interactive data: data asset containing information related to child interactions with social features of the internet connected toy or other entities

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

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

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

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

3.1.5 Data related terms

authentication factor: element used by an entity to proof an identity claim

EXAMPLE: A PIN, a password, a fingerprint, a shared symmetric cryptographic key, an one-time-password generated by a security token, an one-time-password received by E-Mail.

NOTE: An authentication factor can be of the type knowledge, inherence or possession.

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

EXAMPLE: Symmetric keys, private keys.

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

connection data: communicated data that contains information necessary for testing or establishing communication capability via machine interfaces

EXAMPLE: IP address as part of an IP package header.

data: information in digital form

derived token: short term authentication factor generated with the use of a security token

EXAMPLE: A time-based one-time secret which can be used to authenticate an entity, a response to a challenge which can be used authenticate an entity, a HMAC-based one-time password.

NOTE: Derived tokens can be provided by Services or via Accounts in possession of the entity or generated by a security token.

location data: data containing geographical information

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

EXAMPLE: Symmetric keys, private keys

NOTE 1: A password is a cryptographic security parameter.

NOTE 2: Passwords are sometimes chosen to be remembered by humans such as 4-digit PINs.

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

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

public data: data from publicly accessible sources

security token: long term authentication factor of the type possession

EXAMPLE: private key which can be used to authenticate an entity, a smartcard that can be used to authenticate an entity, a long term symmetric key that can be used to authenticate an entity.

targeted modification of stored data: physical modification of data storage that leads to a fully controlled change of the stored data

EXAMPLE: Physical overwrite of storage that stores a user password's reference value with a reference value for a password generated by an attacker.

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

3.1.6 Function assets

connection function: internet connected toy function that is used for testing or establishing communication capability via machine interfaces

EXAMPLE: ICMP, DHCP Discovery.

NOTE: In this context, establishing communication means communication without user-related data and without authentication of the communication partner for the purpose of establishment of a connection.

data communication function: internet connected toy function that communicates data assets to or receives data assets from another architectural component or another product

EXAMPLE 1: Sending data assets to another architectural component.

EXAMPLE 2: Receiving data assets from another product.

data modification function: internet connected toy function that can create, delete or change data assets

EXAMPLE: Storing data created by an external sensing function.

data presenting function: internet connected toy function that grants an entity read access to data or presents data to a user via physical human interface

EXAMPLE 1: Presenting data to a user on a website associated with a RDPS.

EXAMPLE 2: Presenting data on a display, controlling indicator lights.

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

EXAMPLE: Recording video or audio or measuring temperature, pressure or brightness.

internal sensing function: internet connected toy function to measure characteristics of the internet connected toy or parts of it

EXAMPLE: Monitoring unsuccessful authentication attempts.

parental control function: internet connected toy function that enables parents or guardians to control:

- access rights of children on the internet connected toy;
- sources where children can access external content from; or
- persons that can communicate with the child.

security function: internet connected toy function that protects internet connected toy assets

EXAMPLE: Authentication mechanism, integrity protecting secure storage mechanism or input validation mechanism.

3.1.7 Function related terms

access control mechanism: function that enforces an authorisation policy

NOTE: An access control mechanism is a security function.

authentication mechanism: function that verifies an entity's identity claim by using authentication factors of the type inherence, knowledge or possession

NOTE: An authentication mechanism is a security function.

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

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

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

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

bootloader function: function that initiates the execution of other core software at start up

NOTE: A bootloader function is a security function.

confidentiality protecting communication mechanism: function that protects the confidentiality of communicated data

NOTE: A confidentiality protecting communication mechanism is a security function.

confidentiality protecting secure storage mechanism: function that protects the confidentiality of persistently stored data

NOTE: A confidentiality protecting secure storage mechanism is a security function.

configuration function: function that allows to change the configuration of internet connected toy's functions

NOTE: A configuration function is a data modification function that modifies function configuration data.

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

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

cryptographic function: function that performs cryptographic algorithm

NOTE: A cryptographic function is a security function.

cryptographic mechanism: security-related procedure using cryptography

NOTE 1: The term "cryptographic mechanism" is used as an umbrella term covering the categories used in the Agreed Cryptographic Mechanisms [1], including cryptographic algorithms, primitives, schemes, protocols, protocol profiles, cipher suites, modes of operation, constructions and parameter sets.

NOTE 2: The terms "cryptographic primitive", "cryptographic construction", "cryptographic scheme" and "cryptographic protocol" are used consistently with Agreed Cryptographic Mechanisms [1].

NOTE 3: A cryptographic mechanism can be specified at different levels of abstraction. For example, AES is a cryptographic primitive, AES-GCM is a mode of operation / authenticated encryption construction, TLS 1.3 is a protocol, a TLS 1.3 restricted cipher-suite profile is a protocol profile, and TLS_AES_128_GCM_SHA256 is a cipher suite.

cryptographic parameter guessing probability: probability of randomly guessing a valid authentication factor based on the expected number of guesses, the number of possible authentication factors and the number of valid authentication factors

EXAMPLE: For T_{SI} of one day (86 400 seconds), $C_{CP,min}$ of 10 000, only one valid combination at any time and $f_{VA,max}$ of $\frac{3}{3 \times 3s + 3\,600s}$ for a waiting period of one hour after 3 failed attempts and 3 seconds per attempt, the $p_{GRP} = \frac{86\,400s \times 3}{(3 \times 3 + 3\,600)s \times 10\,000} \approx 7,18 \times 10^{-3}$.

NOTE: The p_{GRP} is defined in a way to allow for a tradeoff between complexity of passwords or PINs and restrictions on the number of attempts to enter a password or PIN.

cryptographic property: property provided or supported by a cryptographic mechanism

NOTE 1: Cryptographic properties include, for example, confidentiality, integrity, authenticity, entity authentication, message authentication, key establishment, key confirmation, replay protection, collision resistance, second-preimage resistance, pre-image resistance, signature unforgeability, non-repudiation, forward secrecy and password-verifier protection. Where relevant, a cryptographic property can be expressed using a formal cryptographic notion, for example IND-CPA, IND-CCA, IND-CCA2, EUF-CMA, SUF-CMA or authenticated key exchange security.

NOTE 2: A cryptographic property is distinct from a product-level technical requirement, although it can support such a requirement. For example, a secure communication requirement can rely on cryptographic properties such as confidentiality, integrity and authentication.

data backup mechanism: function that copies data assets to persistent storage of another architectural component or target outside the internet connected toy

NOTE: A data export mechanism can be a data presenting function and/or a data communication function.

data export mechanism: function that exports data assets for persistent storage in another device

NOTE: A data export mechanism can be a data presenting function and/or a internet connected toy function which can communicate internet connected toy data.

data transfer mechanism: function that transfers data assets for persistent storage in another internet connected toy's architectural component or in another device/service

NOTE: A data transfer mechanism is a data communication function.

deletion mechanism: function to delete internet connected toy data on a permanent basis

NOTE: A deletion mechanism is a data modification function.

effective cryptographic security parameter bitlength: base two logarithm of the maximum number of operations to break a cryptographic security parameter security property by brute-force-attacks

EXAMPLE 1: $L_{CP,eff}$ is 192 for a 192-bit perfectly random AES key.

EXAMPLE 2: The $L_{CP,eff}$ is $256/2 = 128$ for a perfectly random 256-bit Elliptic Curve Cryptography (ECC) key.

EXAMPLE 3: The $L_{CP,eff}$ is $0,0235 \times (\log_2(7\,680))^{3,54} \approx 201 > 192$ for a perfectly random 7 680-bit RSA key.

EXAMPLE 4: ML-KEM-512 has $L_{CP,eff}$ of 128 (security category 1, NIST FIPS 203 [i.14]) and ML-DSA-44 has $L_{CP,eff}$ of at least 128 (security category 1 or 2, NIST FIPS 204 [i.15]).

NOTE: Here, the $L_{CP,eff}$ is equal to the key length for perfectly random symmetric cryptographic keys, the half of key length for perfectly random asymmetric cryptographic keys based on Elliptic Curve Cryptography (ECC) and $L_{CP,eff} = 0,0236 \times (\log_2(key\ length))^{3,54}$ for perfectly random asymmetric cryptographic keys for RSA (Rivest-Shamir-Adleman) cryptosystems. The calculation of $L_{CP,eff}$ is based on the recommendations in NIST SP 800-78-5 [i.9]. For ML-KEM and ML-DSA, $L_{CP,eff}$ can be adapted from the "security category", see "security strength" in NIST SP 800-57-1 [i.16], with "security category 1" corresponding to an $L_{CP,eff}$ of 128, "security category 2" corresponding to an $L_{CP,eff}$ of 192 etc.

factory reset function: function that removes all user-related data and sets the architectural components in a factory default state, potentially keeping software updates

NOTE: A factory reset function is a data modification function.

false acceptance rate: frequency at which an unknown entity is incorrectly accepted by an authentication mechanism

NOTE: The FAR is a parameter used to differentiate between authentication strength levels in clause [E.1](#).

false rejection rate: frequency at which a known identity is incorrectly rejected by an authentication mechanism

NOTE: The FRR is a parameter used to differentiate between authentication strength levels in clause [E.1](#).

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

- a modification or creation of internet connected toys' data or functions;
- information intended to inform human users;
- information intended to inform or control devices or services; or
- an action on the physical operational environment.

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

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

- human users;
- devices or services; or
- the physical operational environment.

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

identity: set of attributes related to an entity

NOTE: As defined in ISO/IEC 24760-1 [i.7]:2025 [i.7].

input sanitisation mechanism: function that scans function input data based on a function specific pattern and removes or alters parts, that can lead to incidents

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

NOTE: An input sanitisation mechanism is a security function.

input validation mechanism: function that rejects input data if it does not meet an accepted pattern

EXAMPLE: The input is expected to be the users' year of birth. Data type validation is used to ensure the input to be an integer followed by a range validation checking that the input is between 1900 and the current year.

NOTE: An input validation mechanism is a security function.

integrity protecting communication mechanism: function that protects the integrity of communicated data

NOTE: An integrity protecting communication mechanism is a security function.

integrity protecting secure storage mechanism: function that protects the integrity of persistently stored data

NOTE: An integrity protecting secure storage mechanism is a security function.

logging mechanism: function that ensures storing of audit event data generated by a monitoring mechanism

NOTE: A logging mechanism is a data modification function or a data communication function.

maximal valid derived tokens: maximum number of derived tokens which are considered valid authentication factor at any given time

EXAMPLE 1: $n_{dt,max}$ is 1, where the derived tokens are only generated on demand and invalidated if a new derived token is generated during an other derived tokens T_{VA} .

EXAMPLE 2: $n_{dt,max}$ is $15/1 = 15$ where a derived token is automatically generated every minute and has T_{VA} of 15 minutes.

maximum sustained validation attempt frequency: long term frequency at which an authentication mechanism accepts authentication attempts

EXAMPLE 1: $f_{VA,max}$ is $\frac{5}{5 \times 3s + 3600s} \approx 1,4 \times 10^{-3} \frac{1}{s}$ for 3 s per login attempt + a one-hour waiting period after 5 failed login attempts.

EXAMPLE 2: $f_{VA,max}$ is $\frac{1}{0,1s} = 10 \frac{1}{s}$ for 10 login attempts per second.

EXAMPLE 3: The product $T_{SI} \times f_{VA,max} = 3$, if after three failed attempts, no further attempts can be made.

minimal recommended cryptographic security parameter complexity: number of all possible combinations meeting the minimal recommended number and positions of characters for an authentication mechanisms authentication factor

EXAMPLE 1: $C_{CP,min}$ is 10^5 for a five-digit numerical PIN.

EXAMPLE 2: $C_{CP,min}$ is $9!/(9-5)!$ for an ordered pattern of five non repeating nodes in a 9-node fully connected graph.

EXAMPLE 3: $C_{CP,min}$ is $(26 \times 2 + 10 + 8)^8$ for a password of recommended length of 8 characters from the set of upper and lower case letters, numbers and 8 special characters.

EXAMPLE 4: $C_{CP,min}$ is 2^{2048} for a 2 048-bit response generated by a security token.

monitoring mechanism: function that (frequently) measures metrics of the internet connected toy and generates audit event data

NOTE: A monitoring mechanism is a internal sensing function.

multi factor authentication: authentication method where more than one authentication factor of different types are evaluated by an authentication mechanism

EXAMPLE: Entering a PIN or scanning a Fingerprint in addition to entering an OTP generated by a security token to unlock the front door via the Internet, using a mobile device.

notification mechanism: function that notifies entities on certain events

NOTE: A notification mechanism is a data communication function.

onboarding mechanism: configuration function that is used during the internet connected toy's' initialisation process

NOTE: An onboarding mechanism is a data modification function that modifies function configuration data.

security insurance time: time during which an authentication mechanism is expected to withstand random guessing attacks

NOTE: The T_{SI} is a parameter used to differentiate between authentication strength levels in clause [E.1](#).

single factor authentication: authentication method where only one authentication factor is evaluated by an authentication mechanism

EXAMPLE: Entering a PIN or scanning a Fingerprint to unlock the configuration UI of a internet connected toy.

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

software package verification mechanism: function that verifies the integrity and authenticity of software packages

NOTE: A software package verification mechanism is a security function.

software update mechanism: function that receives and installs software updates

NOTE: A software update mechanism is a data modification function and data communication function where the data are function binary data.

time during which a token is valid: time, after its creation, during which a derived token is accepted as valid by an authentication mechanism

EXAMPLE: An OTP has a time window of 30min after its generation, after which it will no longer be accepted as valid.

3.1.8 Interface

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

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

interface: shared boundary across which the internet connected toy exchanges information

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

EXAMPLE: Web page for remote access.

NOTE: An external client used for remote access providing a logical human interface typically uses a machine interface to communicate with the internet connected toy.

logical interface: interface that does not exist in hardware and can only be used by using another device or a physical interface of a internet connected toy

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

EXAMPLE: Interfaces for USB/Bluetooth®/Ethernet/Wi-Fi®/DECT/DECT-2020 NR or debug ports accessible from outside the internet connected toy.

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

EXAMPLE: Keypad, display, biometric reader, microphone, loudspeaker, (video) camera, touchscreen.

physical interface: interface that is part of the hardware of a internet connected toy

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

3.1.9 Operational environments

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

fully controlled physical operational environment: physical operational environment, where physical access is fully controlled by the guardian or trusted persons

EXAMPLE: Private house or apartment.

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

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

NOTE: Physical operational environment of smartphones and wearables.

operational environment: system used to model to likelihood of incidents depending on the physical operational environment of the internet connected toy, or parts of it, and the logical operational environment of the relevant logical interfaces

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

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

physical operational environment: operational environment determining the physical accessibility of an architectural component

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

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

EXAMPLE: Areas intended for public access.

3.1.10 Users

child: human entity under 14 years of age

guardian: natural or legal entity with responsibility for the child

NOTE: This includes also parents.

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

NOTE 1: This includes all natural entities that interact directly with the internet connected toy as the final product, but not manufactures for integration in other products.

NOTE 2: User can include guardian, child, adult who play and manage their own cybersecurity or adolescent (over the age of 14).

3.2 Symbols

For the purposes of the present document, the following symbols apply:

$C_{CP,min}$	Minimal recommended cryptographic security parameter complexity
$f_{VA,max}$	Maximum sustained validation attempt frequency
$L_{CP,eff}$	Effective cryptographic security parameter bitlength
$n_{dt,max}$	Maximal valid derived tokens
p_{GRP}	Cryptographic parameter guessing probability
T_{SI}	Security insurance time
T_{VA}	Time during which a token is valid

3.3 Abbreviations

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

GENERAL

ACM	Agreed Cryptographic Mechanisms
AES	Advanced Encryption Standard
AES-GCM	Advanced Encryption Standard in Galois/Counter Mode
CMAC	Cipher-based Message Authentication Code
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
ECC	Elliptic Curve Cryptography
EUF-CMA	Existential Unforgeability under Chosen Message Attack
FAR	False Acceptance Rate
FRR	False Rejection Rate
GPS	Global Positioning System
GUI	Graphical User Interface
HMAC	Hash-based Message Authentication Code
ICMP	Internet Control Message Protocol
IND-CCA	Indistinguishability under Chosen-Ciphertext Attack
IND-CCA2	Indistinguishability under adaptive Chosen-Ciphertext Attack
IND-CPA	Indistinguishability under Chosen-Plaintext Attack
IP	Internet Protocol
LED	Light Emitting Diode
MFA	Multi Factor Authentication
OTP	One-Time Password
PIN	Personal Identification Number
PitM	Person in the Middle
RDPS	Remote Data Processing Solution
ROM	Read Only Memory
RSA	Rivest-Shamir-Adleman
SFA	Single Factor Authentication
SUF-CMA	Strong existential Unforgeability under Chosen Message Attack
TLS	Transport Layer Security
UI	User Interface
UPnP	Universal Plug and Play
USB	Universal Serial Bus

COMMUNICATION TYPES

COM	Communication Type
COM.Adjacent	Adjacent Communication
COM.Local	Local Communication
COM.Public	Public Communication
COM.StrictLocal	Strict Local Communication

IMPACT CLASSES

IMP	impact class
IMP.AVAI.LOSS	loss sensitive availability impact class
IMP.AVAI.LOSS.High	loss sensitive availability impact class high
IMP.AVAI.LOSS.Low	loss sensitive availability impact class low
IMP.AVAI.LOSS.Medium	loss sensitive availability impact class medium
IMP.AVAI.TIME	time sensitive availability impact class
IMP.AVAI.TIME.High	time sensitive availability impact class high
IMP.AVAI.TIME.Low	time sensitive availability impact class low
IMP.AVAI.TIME.Medium	time sensitive availability impact class medium
IMP.CONF	confidentiality impact class
IMP.CONF.High	confidentiality impact class high
IMP.CONF.Low	confidentiality impact class low

IMP.CONF.Medium confidentiality impact class medium
IMP.FH impact class for function whose use can cause harm
IMP.FH.CCON function which can communicate confidential data impact class
IMP.FH.DSN function whose use can impact the availability of other devices, services or networks impact class
IMP.FH.DSN.High function whose use can impact the availability of other devices, services or networks impact class high
IMP.FH.DSN.Low function whose use can impact the availability of other devices, services or networks impact class low
IMP.FH.DSN.Medium function whose use can impact the availability of other devices, services or networks impact class medium
IMP.FH.High function whose use can cause harm impact class high
IMP.FH.Low function whose use can cause harm impact class low
IMP.FH.Medium function whose use can cause harm impact class medium
IMP.FH.MINT function which can modify integrity relevant data impact class
IMP.FH.SP function whose use can impact the safety or privacy of human entities impact class
IMP.INT integrity impact class
IMP.INT.High integrity impact class high
IMP.INT.Low integrity impact class low
IMP.INT.Medium integrity impact class medium

INTERFACES

IF interface
IF.Any unspecified interface
IF.Human human interface
IF.HumanLogical logical human interface
IF.HumanPhysical physical human interface
IF.Logical logical interface
IF.Machine machine interface
IF.Physical physical interface

OPERATIONAL ENVIRONMENTS

LOE logical operational environment
POE physical operational environment
POE.Any unspecified physical operational environment
POE.Confined confined operational environment
POE.FullyControlled fully controlled physical operational environment
POE.Mobile mobile operational environment
POE.PartiallyControlled partially controlled physical operational environment
POE.Stationary stationary operational environment
POE.Uncontrolled uncontrolled physical operational environment

PROTECTION MEASURE STRENGTH LEVEL

AUTH.Basic authentication - protection strength level basic
AUTH.Enhanced authentication - protection strength level enhanced
AUTH.Normal authentication - protection strength level normal
AUTH.Strong authentication - protection strength level strong
CONF.COM.Basic communication of confidential data - protection strength level basic
CONF.COM.Enhanced communication of confidential data - protection strength level enhanced
CONF.COM.Normal communication of confidential data - protection strength level normal
CONF.COM.Strong communication of confidential data - protection strength level strong
CONF.SSM.Basic confidential persistent storage - strength level basic
CONF.SSM.Enhanced confidential persistent storage - strength level enhanced
CONF.SSM.Normal confidential persistent storage - strength level normal
CONF.SSM.Strong confidential persistent storage - strength level strong
INT.COM.Basic communication of integrity relevant data - protection strength level basic
INT.COM.Enhanced communication of integrity relevant data - protection strength level enhanced
INT.COM.Normal communication of integrity relevant data - protection strength level normal
INT.COM.Strong communication of integrity relevant data - protection strength level strong

INT.SSM.Basic integrity protecting persistent storage - strength level basic
 INT.SSM.Enhanced integrity protecting persistent storage - strength level enhanced
 INT.SSM.Normal integrity protecting persistent storage - strength level normal
 INT.SSM.Strong integrity protecting persistent storage - strength level strong
 INT.SW.VER.Basic software package integrity verification - strength level basic
 INT.SW.VER.Enhanced software package integrity verification - strength level enhanced
 INT.SW.VER.Normal software package integrity verification - strength level normal
 INT.SW.VER.Strong software package integrity verification - strength level strong
 N/A not applicable

4 Product context

4.1 Product functions

4.1.1 Function assets

The present document addresses the following function assets of internet connected toy:

- connection function
- data communication function
- data modification function
- data presenting function
- external sensing function
- internal sensing function
- parental control function
- security function

NOTE 1: A detailed mapping from the listed function assets to their impact classes is provided in clause [D.2](#).

NOTE 2: Functions in a real internet connected toy can fall under several function assets.

4.1.2 Data assets

The function assets might process the following data assets of internet connected toy:

- activity data
- audit event data
- authorisation policy data
- cryptographic security parameter
- device identifier data
- entity's location data
- function binary data
- function configuration data
- identity data for authentication
- logging data

- network status data
- personal contact data
- personal notes data
- private audio data
- private video data
- public data asset
- real-time data
- social interactive data
- software package
- state data

NOTE 1: A detailed mapping from the listed data assets to their impact classes is provided in clause [D.1](#).

NOTE 2: Data in a real internet connected toy can fall under of several data assets.

4.2 Product architecture

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

NOTE 1: It is possible that a internet connected toy consists of only one hardware architectural component.

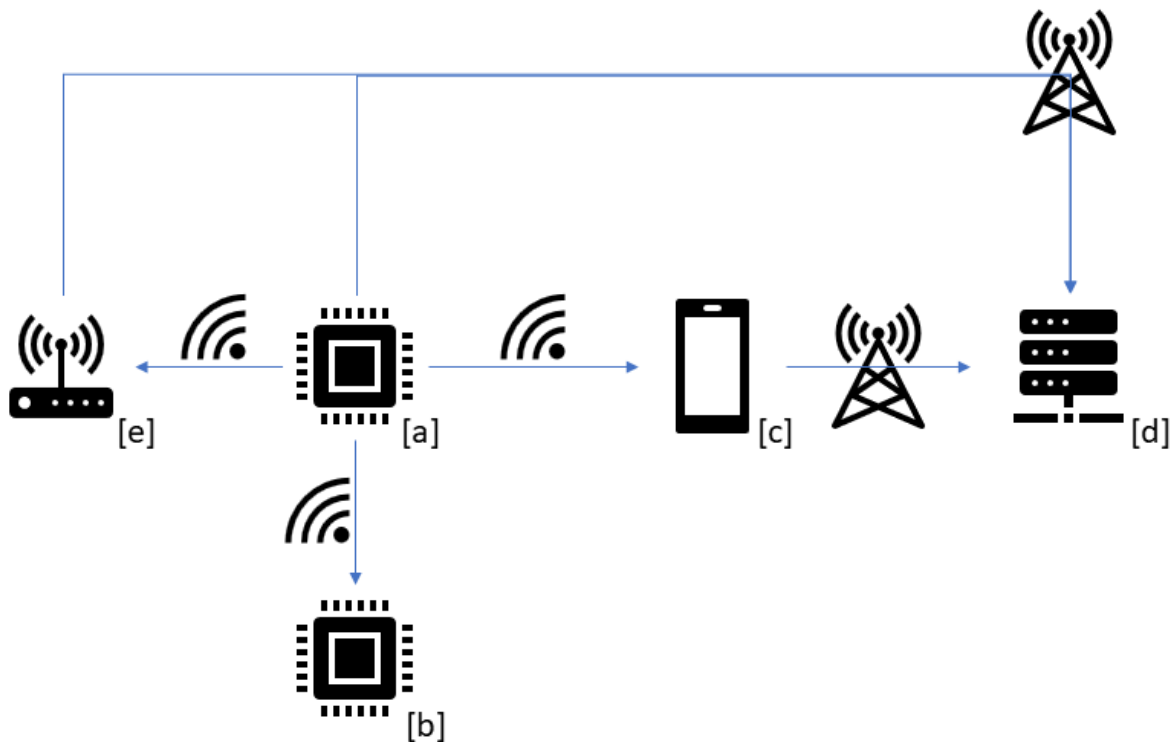


Figure 1: Architectural components and possible connections between them

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

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

NOTE 2: Not all subsets of the internet connected toy's architectural components in this example are necessary for falling into the scope of the present document.

4.3 Operational environment

4.3.1 General description

Void.

4.3.2 Physical/Hardware environment

The following physical operational environments for:

- any hardware architectural component of the internet connected toy; and
- any software architectural component's host device where it is intended or reasonably foreseen to be installed;

are addressed:

- **fully controlled physical operational environment** - POE.FullyControlled;
- **partially controlled physical operational environment** - POE.PartiallyControlled; and
- **mobile operational environment** - POE.Mobile,

by the present document.

4.3.3 Logical/Software environment

For the logical operational environment, the present document addresses the following digital communication types for any architectural component of the internet connected toy:

- **public communication** - COM.Public;
- **adjacent communication** - COM.Adjacent;
- **local communication** - COM.Local; and
- **strict local communication** - COM.StrictLocal.

4.3.4 Connectivity aspects

The following interfaces, on which physical and digital communication builds upon, are addressed by the present document:

- **human interface** - IF.Human;
- **machine interface** - IF.Machine;

- **logical interface** - IF.Logical; and
- **physical interface** - IF.Physical.

4.4 Distribution of security functions

The present document addresses the distribution of security functions among the internet connected toy and other products with digital elements in the internet connected toy's context (e.g. host devices for internet connected toy's software architectural components) by the following expressions used to formulate the technical requirements specifications in clause [5](#).

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

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

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

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

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

Situations where the internet connected toy itself does not provide security functions that are required to be used or supported by the internet connected toy and other products with digital elements in the internet connected toy's context do not provide those security functions, are addressed in the requirement [USERNOT-NOSECFUC] in clause [5.2.1](#).

4.5 Users

The present document addresses internet connected toy having the following using entities:

- Consumers
- Manufactures for integration in other products with digital elements intended for consumers

4.6 Use cases

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

5 Technical requirements for products

5.1 Introduction - Applicability of the requirements

The technical requirements of the present document apply under the product context described in clause [4](#), which shall be in accordance with its intended use. The product shall comply with all applicable technical requirements of the present document at all times when operating in its product context.

NOTE: The applicability of technical requirements is based on the product context specific to the product such as specific capabilities or specific groups of users of the product. The applicability conditions are explicitly stated within the technical requirements.

The application details of some of the technical requirements depend on impact classes for internet connected toy functions and data. The impact classes shall be assigned in accordance with:

- clause [D.1](#) for data assets; and
- clause [D.2](#) for function assets.

5.2 Appropriate level of cybersecurity

5.2.0 Introduction on appropriate level of cybersecurity requirements

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (1).

5.2.1 [USERNOT-NOSECFUC] User notifications on not available security functions

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

5.2.2 [USERNOT-SECREL] Language and representation for security-related user notifications

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

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

5.2.3 [GUI-SECCONF] Visual representation of security-related configuration via GUIs

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

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

5.2.4 [BACKUP-TRANS] Data transfer mechanisms for loss sensitive data

The internet connected toy shall support data transfer mechanisms for all loss sensitive data persistently stored at the internet connected toy.

5.2.5 [BACKUP-AUTOTRANS] Automatic data transfer mechanisms for loss sensitive data

The internet connected toy shall support automatic data transfer mechanisms for all loss sensitive data of impact class [IMP.AVAILLOSS.Medium] or higher persistently stored at the internet connected toy.

5.2.6 [BACKUP-EXPORT] Data export mechanisms for loss sensitive data

Where the internet connected toy is intended to be installed or maintained by a consumer for private usage, the internet connected toy shall support data export mechanisms for all loss sensitive data of impact class

[IMP.AVAIL.LOSS.Medium] or higher persistently stored at the internet connected toy such that the guardian can export the data stored at an architectural component:

- centrally at the architectural component, or
- centrally at another architectural component.

5.3 No known exploitable vulnerabilities

5.3.0 Introduction on no known exploitable vulnerabilities

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (a).

5.3.1 [NKEV-MKAV] No known exploitable vulnerabilities

The internet connected toy shall prior to making available on the market not contain known exploitable vulnerabilities, except for those known exploitable vulnerabilities that are subject to a vulnerability handling process for the internet connected toy.

NOTE 1: The known exploitable vulnerabilities that occur after making the internet connected toy available on the market are subject to the vulnerability handling in prEN 40000-1-3 [i.5]).

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

5.3.2 [NKEV-INIT-UDP] Initial security update before or during first use

The internet connected toy's architectural components shall:

- request information on the availability of security update packages; and
- notify guardians when security update packages are available; and
- (if not blocked by the entity that puts the architectural component into first use) request and install available security update packages

before or during first use.

5.4 Secure by default configuration

5.4.0 Introduction on secure by default configuration

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (b).

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

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

- the authentication mechanisms strengths specified in clause [E.1.1](#); and
- the minimal authentication mechanisms' strength determined by table [2](#);

except for connection functions.

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

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

Where:

- the internet connected toy has the capability to connect to a public network; and
- no time sensitive function with IMP.AVAI.TIME.High is provided by an architectural component; and
- automatic installation of updates does not create an unacceptable risk to essential function availability or safety;

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

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

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

5.4.3 [SDC-SUM-NOTIF] Default configuration of update notifications

The internet connected toy shall by default be configured to use automated notification of its users, when updates of the internet connected toy's software are available.

NOTE: The support of update notification is addressed in [SU-NOTIF].

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

All hardware architectural components of the internet connected toy shall provide a factory reset mechanism that allows a guardian to restore the default state, including the secure deletion of all user-related data, installed applications, and configurations deviating from the default state.

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

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

5.4.5 [SDC-PARCONT] Default configuration for parental control

The internet connected toy shall by default be configured to:

- deny children access to security relevant configuration function; and
- restrict the sources where children can access external content from to trusted sources; and
- restrict entities that can communicate with the child to trusted entities.

EXAMPLE 1: The internet connected toy is used by the child without any prior configuration by a guardian. Access to communication with others and external data is not possible and cannot be enabled by the child.

EXAMPLE 2: The internet connected toy is initially configured by the guardian. The guardian determines which external content the child is allowed to access, with the internet connected toy offering different levels based on the child's age. The trusted entities with which the child is allowed to communicate are also determined by a guardian.

NOTE: The requirement [SDC-PARCONT] addresses the default configuration of parental control functions. The support of parental control functions is addressed in [PARCONT].

5.4.6 [SDC-MON-HANDLE] Handling of events by default

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

- a logging mechanism; or
- where the architectural component does not support public communication, a data transfer mechanism,

to handle every audit event data created by a monitoring mechanism.

5.4.7 [CRY-GENERAL] General requirements related to cryptography

The internet connected toy shall comply with the technical requirements provided in annex [K](#).

5.4.8 [CRY-CCK-PRE-LEN] Key size of preinstalled long term confidential cryptographic keys

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

- listed in Agreed Cryptographic Mechanisms [1]; or
- provide a minimum security strength of 112 bit.

5.4.9 [CRY-CCK-GEN] Default key size of generated long term confidential cryptographic keys

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

- listed in Agreed Cryptographic Mechanisms [1]; or
- provide a minimum security strength of 112 bits.

5.4.10 [CRY-PW-PRE-COM] Complexity of preinstalled passwords

The internet connected toy shall only provide preinstalled passwords:

- that meet the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) determined by the corresponding authentication mechanisms' usage according to table [2](#) and corresponding assessments; and
- that are either:
 - individual per internet connected toy and not derivable via publicly available information; or
 - random per internet connected toy.

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

The internet connected toy shall by default only generate passwords:

- that meet the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) determined by the corresponding authentication mechanisms' usage according to table [2](#) and corresponding assessments; and
- that are random.

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

The internet connected toy shall only use user chosen passwords that meet the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) determined by the corresponding authentication mechanisms' usage according to table 2 and corresponding assessments, except for user chosen passwords where the user explicitly confirms their usage after a warning by the internet connected toy.

5.5 Security updates

5.5.0 Introduction on security updates

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (c).

5.5.1 [SU-SUPPORT] Secure software update mechanism

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

NOTE 1: A mobile application, as part of a internet connected toy, can be developed and distributed, such that it will receive security updates via the software update mechanism of the host system's application distribution platform. Thus, the internet connected toy supports a software update mechanism for the mobile application.

NOTE 2: A device, as part of a internet connected toy, can be developed such that its entire software can be updated via its core software's software update mechanism. Thus, the device supports a software update mechanism for its software. In this case the software update mechanism is provided by the core software of the device.

NOTE 3: Part of the internet connected toy's software can be immutable due to the technology which is used to store its executable code (e.g. software installed in a ROM).

5.5.2 [SU-PROVIDE] Secure software update mechanism for core components

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

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

5.5.3 [SU-AUTO] Automated security updates

Where

- the internet connected toy has the capability to connect to a public network; and
- automated installation of updates does not create an unacceptable risk to essential function availability or safety,

the internet connected toy shall support the automated security update of its software within an appropriate time frame.

NOTE 1: Automatic installation of security updates could create an unacceptable risk to essential function availability or safety in situations where installation could interrupt availability relevant essential functions or create safety risks in foreseeable emergency use (e.g. delaying egress during a fire alarm, preventing prompt access for emergency responders, or preventing timely arming/disarming/panic activation during an intrusion event).

NOTE 2: Where automated security updates are not supported, the user will typically be informed (e.g. via the internet connected toy's user documentation).

NOTE 3: The appropriateness of timeframes between the existence of a security update package, its transfer to the architectural component and its automated installation depends on the attack surface the architectural component is exposed to, the criticality of potential vulnerabilities addressed by a security update, the impact class IMP.AVAI.TIME of affected time sensitive functions, the impact class IMP.INT of affected integrity relevant functions and integrity relevant data. The corresponding behaviour of an architectural component can amongst other be specified by appropriate fixed values (e.g. always download security update packages within one day, perform the automated security update installation two hours after the download is finished) or by parameters related to a specific security update package (e.g. download security update package immediately, perform the automated update installation immediately after the download is finished for critical security updates where integrity protection is crucial or download security update package within one week, perform the automated update installation within one week after the download is finished for uncritical security updates that might affect time sensitive functions).

5.5.4 [SU-DISABLE-AUTO] Option to disable automated security updates

Where the internet connected toy provides mechanisms for automated security update of internet connected toy's software operated by guardians, the internet connected toy shall provide a clear and easy-to-use option for guardians to disable those mechanisms.

5.5.5 [SU-POSTPONE-AUTO] Option to postpone automated security updates

Where the internet connected toy provides mechanisms for automated security update of internet connected toy's software operated by guardians, the internet connected toy shall provide an option for guardians to temporarily postpone the automated installation of updates.

NOTE: The time to postpone the automated installation of security updates can be set by the guardian.

5.5.6 [SU-NOTIF] Update notifications

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

5.6 Authentication and access control

5.6.0 Introduction on authentication and access control

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (d).

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

The internet connected toy shall use access control mechanisms to control entities' use of functions whose use can cause harm, where the applicability of this requirement is determined by table 1 except for connection functions.

Table 1: Assignment for access control mechanisms

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

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

- factory reset function;
- functions configured by parental control functions.

5.6.2 [PARCONT] Support of parental control

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

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

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

Where the authorisation policy restricts permissions, the internet connected toy shall support authentication mechanisms, to authenticate entities using functions whose use can cause harm before generating function output, where:

- the authentication mechanisms strengths' are specified in clause [E.1.1](#); and
- the minimal required authentication strength is determined by table [2](#),

except for connection functions.

Table 2: Assignment for authentication mechanisms strengths

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

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

factory reset function;

functions configured by parental control functions.

5.6.4 [AUTHZ-LP] Least privilege in authorisation policies

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

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

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

5.6.5 [AUTHZ-R] Revocability of granted permissions

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

EXAMPLE: A guardian can revoke permissions granted to the child.

5.6.6 [AUTHZ-PC] Authorisation policies for parental control

The internet connected toy shall use an authorisation policy that:

- can differentiate between a guardian and a child and;
- does not allow a child to use parental control functions.

5.7 Confidentiality protection

5.7.0 Introduction on confidentiality protection

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (e).

5.7.1 [CONF-SSM] Confidentiality protecting persistent storage for confidential data

The internet connected toy shall use confidentiality protecting secure storage mechanisms for persistently stored confidential data, where the mechanisms' strength are specified in clause [E.3.1](#) and the minimal required mechanisms' strength are determined by table [3](#).

NOTE: Typically, encryption/decryption keys for storage encryption are stored such that they cannot be extracted. Corresponding protection measures are subject to confidential persistent storage - strength level strong.

Table 3: 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 component that persistently stores confidential data	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

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

- which is persistently stored on non-removable storage.

5.7.2 [CONF-COM] Communication of confidential data

The internet connected toy shall use confidentiality protecting communication mechanisms to protect the confidentiality of communicated confidential data, where the corresponding confidentiality protection measures strengths are specified in clause [E.3.3](#) and the minimal required confidentiality protection measures' strength are determined by table [4](#).

NOTE: The internet connected toy can communicate data with other devices or services and between architectural components, e.g. between a internet connected toy's hardware architectural component and its RDPS.

Table 4: 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[*]
For protection measures labelled with [*], it is not required that the internet connected toy uses confidentiality protecting communication mechanisms for confidential data: • which is used as connection data.					

5.8 Integrity protection

5.8.0 Introduction on integrity protection

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (f).

5.8.1 [INT-SSM] Integrity protecting persistent storage for integrity relevant data

The internet connected toy shall use integrity protecting secure storage mechanisms for persistently stored integrity relevant data, where the mechanisms' strength are specified in clause [E.2.1](#) and the minimal required mechanisms strength are determined by table [5](#).

Table 5: Assignment for integrity protecting secure storage mechanisms

		Integrity impact class for persistently stored integrity relevant data		
		IMP.INT.Low	IMP.INT.Medium	IMP.INT.High
Attack Surface determined by POE of the architectural component that persistently stores integrity relevant data	POE.FullyControlled	N/A	N/A	N/A
	POE.PartiallyControlled	N/A	INT.SSM.Basic[*]	INT.SSM.Normal
	POE.Mobile	INT.SSM.Basic[*]	INT.SSM.Normal	INT.SSM.Enhanced
For protection measures labelled with [*], it is not required that the internet connected toy uses integrity protecting persistent storage for integrity relevant data: • which is persistently stored on non-removable storage.				

5.8.2 [INT-COM] Communication of integrity relevant data

The internet connected toy shall use integrity protecting communication mechanisms to protect the integrity of communicated integrity relevant data, where the corresponding integrity protection measures strengths are specified in clause [E.2.3](#) and the minimal required integrity protection measures' strength are determined by table [6](#).

NOTE: The internet connected toy can communicate data with other devices or services and between architectural components, e.g. between a internet connected toy's hardware architectural component and its RDPS.

Table 6: 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[*]
For protection measures labelled with [*], it is not required that the internet connected toy uses integrity protecting communication mechanisms of strength higher than INT.COM.Basic to protect the integrity of communicated integrity relevant data:					
• which is used as connection data.					

5.8.3 [INT-SWPCK] Software package verification

The internet connected toy shall use software package verification mechanisms to verify the integrity and authenticity of software packages prior to installation where the software package verification mechanism's strength levels are specified in clause [E.2.5](#) and where the minimal software package verification mechanism's strength is determined by table [7](#).

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

Table 7: Assignment of the software package verification mechanism's strength levels for the 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 component over which the software package is received	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

5.9 Data minimisation

5.9.0 Introduction on data minimisation

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (g).

5.9.1 [DMIN-DJST] Minimise processed data

The internet connected toy shall only process data which are adequate, relevant and limited to its intended purpose.

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

5.10 Availability protection

5.10.0 Introduction on availability protection

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (h).

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

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

5.10.2 [AVAI-TIME-NETW] Local operation

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

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

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

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

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

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

5.10.4 [AVAI-TIME-OUTA-NOT] Notify non-availability

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

EXAMPLE: A cloud RDPS recognises a non-availability of a hardware architectural component and sends a notification to the guardian.

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

5.10.5 [AVAI-TIME-PREV-NOT] Notify upcoming limitation

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

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

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

5.10.6 [AVAI-TIME-NET-PRIO] Network prioritisation

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

- such that these functions are prioritised according to their time sensitive availability impact class (IMP.AVAI.TIME); or
- such that functions are prioritised according to user decisions or configuration.

5.10.7 [AVAI-TIME-RES-PRIO] Power resource prioritisation

Where:

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

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

- such that these functions are prioritised according to their time sensitive availability impact class (IMP.AVAI.TIME); or
- such that functions are prioritised according to user decisions or configuration.

5.10.8 [AVAI-TIME-DOS-RATE] Incoming rate limiting

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

5.10.9 [AVAI-SUM-SCHEDULE] Scheduling of updates

Where:

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

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

5.11 Non-interference

5.11.0 Introduction on non-interference

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (i).

5.11.1 [NOINF-AMP] Amplification control

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

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

5.12 Attack surface minimisation

5.12.0 Introduction on attack surface minimisation

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (j).

5.12.1 [LAS-INVAL] Validation of external data input

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

- COM.Local; and
- COM.Adjacent; and
- COM.Public.

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

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

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

5.12.2 [LAS-INSAN] Sanitisation of external data input

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

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

5.12.3 [LAS-PHY-INF] Only necessary physical interfaces

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

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

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

5.12.5 [LAS-APP] Only necessary apps by default

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

5.12.6 [LAS-SBOOT] Secure boot

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

NOTE 1: The requirement corresponds to the verified boot capability in ETSI EN 304 623 [i.6].

NOTE 2: The internet connected toy can provide a management mechanism by which the material used for verifying core software can be changed by at least, but not limited to, the authorised guardian.

NOTE 3: The verification can be based on cryptographic signatures, hashes or measured boot.

5.13 Exploit mitigation

5.13.0 Introduction on exploit mitigation

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (k).

5.13.1 [PRIV-DATA-HIGH] Privileged access on impact class high data assets

The internet connected toy's architectural components shall use mechanisms to ensure that privileges to access architectural components':

- confidential data with [IMP.CONF.High]; and
- integrity relevant data with [IMP.INT.High],

for processes running on the same hardware, are only assigned where necessary for the internet connected toy's intended purpose.

NOTE: This requirement does not prohibit transfer of confidential data or integrity relevant data.

5.13.2 [PRIV-FUNC-HIGH] Privileged access on impact class high function assets

The internet connected toy's architectural components shall use mechanisms to ensure that privileges to access processes implementing architectural components':

- time sensitive function with [IMP.AVAI.TIME.High]; and
- integrity relevant function with [IMP.INT.High]; and
- function, whose use can cause harm with [IMP.FH.High],

for processes running on the same hardware, are only assigned where necessary for the internet connected toy's intended purpose.

5.14 Monitoring

5.14.0 Introduction on monitoring

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (l).

5.14.1 [MON-LOW] Events to log for low risk internet connected toy

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

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

5.14.2 [MON-MEDIUM] Events to log for medium risk internet connected toy

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

- unsuccessful authentication attempt;
- change of configuration affecting core software;
- starts, shutdowns or other changes of operational states of core software;
- errors of the core software;
- unsuccessful attempt of an identity to gain additional privileges;
- unsuccessful attempt of an identity to access a data asset or function asset.

5.14.3 [MON-HIGH] Events to log for high risk internet connected toy

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

- every authentication attempt;
- change of configuration affecting core software;
- starts, shutdowns or other changes of operational states of core software;
- change of configuration affecting application software that realise functions whose use can cause harm of impact class high;
- starts, shutdowns or other changes of operational states of application software who realise function whose use can cause harm of impact class high;
- errors of the core software;
- errors of the application software who realise function whose use can cause harm of impact class high;
- every attempt of an identity to gain additional privileges;
- every attempt of an identity to access a data asset or function asset.

5.14.4 [MON-HANDLE] Handling of events

The internet connected toy shall support:

- a logging mechanism; or
- where the architectural component does not support public communication, a data transfer mechanism

to handle every audit event data generated by a monitoring mechanism.

NOTE 1: Required audit event data are listed in [MON-LOW], [MON-MEDIUM] or [MON-HIGH].

NOTE 2: Audit event data transferred to this architectural component from another architectural component also have to be processed.

5.14.5 [LOG-TIME] Timestamps for logs

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

5.14.6 [LOG-TIME-HIGH] Real-time timestamps for logs

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

5.14.7 [LOG-STORE-MEDIUM] Logfile persistence for medium risk internet connected toy

Where the internet connected toy has a function, whose use can cause harm of impact class medium as its highest function impact class, the internet connected toy shall support logging mechanisms to store every audit event data:

- for at least 7 days under normal conditions; or
- until at least 100 further logging data have been created for the same architectural component; or
- until the guardian is notified about the upcoming deletion or rotation;

before deletion or rotation of logging data.

NOTE 1: When the maximum number of events is reached, the oldest logging data of a given type are rotated.

NOTE 2: Higher default values for the storage duration or the maximum number of stored logging data are encouraged.

NOTE 3: Audit event data created by an architectural component can be persistently stored on another architectural component.

5.14.8 [LOG-STORE-HIGH] Logfile persistence for high risk internet connected toy

Where the internet connected toy has a function, whose use can cause harm of impact class high as its highest function impact class, the internet connected toy shall support logging mechanisms to store every audit event data:

- for at least 28 days under normal conditions; or
- until at least 1 000 further logging data have been created for the same architectural component; or
- until the guardian is notified about the upcoming deletion or rotation;

before deletion or rotation of logging data.

NOTE 1: When the maximum number of events is reached, the oldest logging data of a given type are rotated.

NOTE 2: Higher default values for the storage duration or the maximum number of stored logging data are encouraged.

NOTE 3: Audit event data created by an architectural component can be persistently stored on another architectural component.

5.14.9 [LOG-CONFIG] Configuration of logging mechanisms

Where the internet connected toy uses logging mechanisms the internet connected toy shall provide a clear and easy to use option for users to disable those mechanisms.

5.15 Factory reset and data portability

5.15.0 Introduction on factory reset and data portability

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (m).

5.15.1 [DLM-PERM] Permanent removal of user-related data

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

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

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

6 Assessment criteria for compliance with technical requirements

6.1 General

This clause provides objective and reproducible assessment criteria to determine whether a product complies with the technical security requirements of clause 5.

For each cybersecurity requirements defined in clause 5, the following clauses specify assessment criteria to determine if the technical requirement is met.

In order to assess the compliance with the requirements listed in clause 5 of the present document, the assessment procedures described in clause 6 are to be followed. When performing assessments, the distribution of security functions (see clause 4.4) are to be considered, including whether the product provides security functions itself, demands them from other products with digital elements within its context, or supplies them to other products with digital elements.

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

- are covering the same assessment activities as described in clause 6; and
- are valid for the moment of the assessment to be performed under clause 6.

those existing evidences can be used for the "assessment verdict" and as "assessment evidence".

The assessment criteria for each security requirements are described in a structured manner, as follows:

- **Assessment reference:** Refers to the identifier of the concerned technical requirement.
- **Assessment objective:** Defines the security property or capability that shall be verified, ensuring that the assessment remains focused on the intent of the requirement.
- **Assessment preparation:** Describes the environment, setup, and preconditions required before executing the test with a view to guaranteeing consistent evaluation results. It includes the following elements as applicable:
 - Test environment: Describe the hardware, software, and network setup used for the assessment, including versions, topology, and any relevant dependencies.
 - Preconditions: Specify any configurations, credentials, or operational states that should be established before the test (e.g. product initialised, certificates loaded, user roles created).
 - Required tools: Identify the tools or software necessary to perform the assessment (e.g. vulnerability scanners, protocol fuzzers, traffic analysers, static code analysers, cryptographic test suites).
 - Required information/documentation for the assessment: Specify all information that is necessary to perform the assessment.

- Reference any vendor provided setup guides, configuration instructions, or operational manuals, as well as any relevant standards or technical notes, that define how the product shall be configured or operated for the assessment.
- **Assessment activities:** Provides execution steps to be performed such that the same assessment verdict would be reached when repeating these steps now or at a later point in time. Assessment activities may include, as applicable:
 - Review information/documentation for the assessment to confirm that the described implementation matches the requirement (e.g. verify that the security architecture document specifies TLS 1.2 or higher for all external interfaces, or that the password policy aligns with the defined threshold).
 - Perform security functional tests to verify the completeness and correctness of the information/documentation for the assessment.
 - Perform security functional or penetration tests to verify that implemented controls are correctly implemented e.g. to prevent unauthorised access or data modification (e.g. via attempting to log in with invalid credentials to test lockout enforcement or trying to modify protected configuration files without administrative privileges).
 - Analyse code or binaries to identify potential security weaknesses or misconfigurations (e.g. perform static analysis to detect hardcoded credentials or use dynamic analysis tools to identify buffer overflow or injection vulnerabilities).
 - Inspect configurations to ensure that required security parameters are correctly applied (e.g. check that weak cipher suites are disabled, two factor authentication is enabled, and least privilege access controls are configured in the system).
 - Observe runtime behaviour to confirm that protections such as encryption, authentication, and integrity verification operate as intended (e.g. monitor network traffic to ensure data in transit is encrypted or observe system logs to verify successful validation of digital signatures during startup).
- **Assessment verdict:** Defines the pass/fail criteria.
 - **Pass:** The assessment is considered passed if the product demonstrably fulfils the requirement and meets the defined security thresholds. Examples of such thresholds include:
 - Minimum cryptographic strength (e.g. AES 128 or higher);
 - Password policy limits (e.g. minimum of 12 characters);
 - Login protection mechanisms (e.g. account lockout after five consecutive failed attempts);
 - Resistance to a specified attack potential (e.g. equivalent to CSA High/AVA_VAN.3 or higher).
 - **Fail:** The assessment is considered failed if the requirement is not fulfilled, or if the defined security thresholds are not achieved (e.g. insufficient key length, missing authentication enforcement, or inadequate resistance to the required attack potential).
- **Assessment evidence:** Defines the artefacts and documentation collected to demonstrate that the requirement has been assessed and fulfilled. The evidence shall be sufficient to enable independent verification of the assessment results and to demonstrate compliance with the relevant CRA essential requirements. The supporting evidence include, where applicable:
 - Test or assessment reports showing the steps performed and results obtained;
 - Logs, configuration files, or audit traces demonstrating the implementation of the requirement;
 - Screenshots, captures, or console outputs confirming the correct execution or protection behaviour;
 - Relevant vendor or design documentation describing the applied security measures.

6.2 Appropriate level of cybersecurity

6.2.1 Assessment criteria for [USERNOT-NOSECFUC]

Assessment reference:

[\[USERNOT-NOSECFUC\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [USERNOT-NOSECFUC]

Assessment preparation:

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

- a list of internet connected toy's architectural components;
- for each architectural component:
 - a list of security functions that are supposed to be used or supported by the architectural component but not provided by the architectural component
 - a description of the (external) component that is expected to provide the security functions that are supposed to be used or supported but not provided by the architectural component
 - a description of the mechanisms to detect and notify the guardian when those functions are not available

Assessment activities:

- The internet connected toy's conformity to [USERNOT-NOSECFUC] shall be validated based on the documentation.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [USERNOT-NOSECFUC].

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation.

6.2.2 Assessment criteria for [USERNOT-SECREL]

Assessment reference:

[\[USERNOT-SECREL\]](#)

Assessment objective:

The assessment covers:

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

Assessment preparation:

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

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

The following test setups shall be prepared:

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

Assessment activities:

- The internet connected toy's conformity to [USERNOT-SECREL] shall be validated based on the documentation.
- The correctness of the implementation shall be verified by inspecting for each used user notification mechanism for security-related notifications whether:
 - one security-related notification is clear, understandable, intelligible, legible and can be easily understood by users; and
 - (where other notifications are possible), the representation of security-related notifications is clearly distinguished from other notifications.

Assessment verdict:

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each used user notification mechanism for security-related notifications.

6.2.3 Assessment criteria for [GUI-SECCONF]

Assessment reference:

[\[GUI-SECCONF\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [GUI-SECCONF];

- a functional sufficiency assessment concerning [GUI-SECCONF] for each internet connected toy's GUI for security-related configuration function.

Assessment preparation:

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

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

The following test setups shall be prepared:

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

Assessment activities:

- The internet connected toy's conformity to [GUI-SECCONF] shall be validated based on the documentation.
- The correctness of the implementation shall be verified by inspecting for each internet connected toy's GUI for security-related configuration function whether:
 - the visual representation of security-related configuration options is clearly visual distinguished from other configuration options; and
 - the consequences of one security-related configuration option is communicated in a clear, understandable, intelligible, legible manner and can be easily understood by users; and
 - the change of one security-related configuration is clearly highlighted visually.

Assessment verdict:

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each GUI for security-related configuration function.

6.2.4 Assessment criteria for [BACKUP-TRANS]

Assessment reference:

[\[BACKUP-TRANS\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [BACKUP-TRANS];
- a functional completeness assessment on the internet connected toy capabilities that are addressed by [BACKUP-TRANS];
- a functional sufficiency assessment of each data transfer mechanisms used by the internet connected toy to fulfil [BACKUP-TRANS].

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of internet connected toy's architectural components;
- for each architectural component:
 - a list of loss sensitive data persistently stored at the architectural component;
 - for each loss sensitive data persistently stored at the architectural component:
 - a description of corresponding data transfer mechanism including possible transfer destinations.

The following test setups shall be prepared:

- for each architectural component, a test setup based on a sample internet connected toy in default configuration for identifying:
 - loss sensitive data persistently stored at the architectural component; and
- for each documented data transfer mechanism, a test setup to trigger the transfer and receive loss sensitive data.

Assessment activities:

- The internet connected toy's conformity to [BACKUP-TRANS] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by:
 - an inspection of the internet connected toy's physical human interfaces for persistently stored loss sensitive data;
 - a scan of the internet connected toy's logical interfaces for persistently stored loss sensitive data.
- For each documented data transfer mechanism, its correct implementation shall be verified triggering the transfer and receiving loss sensitive data.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [BACKUP-TRANS]; and
- the verification of the correctness and completeness of the documentation was successful; and
- the verification of the correct implementation of each data transfer mechanism was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;

- descriptions of the performed tests and records of performed tests to verify the correctness and completeness of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each data transfer mechanism

6.2.5 Assessment criteria for [BACKUP-AUTOTRANS]

Assessment reference:

[\[BACKUP-AUTOTRANS\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [BACKUP-AUTOTRANS];
- a functional completeness assessment on the internet connected toy capabilities that are addressed by [BACKUP-AUTOTRANS];
- a functional sufficiency assessment of each automatic data transfer mechanisms used by the internet connected toy to fulfil [BACKUP-AUTOTRANS];

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of internet connected toy's architectural components;
- for each architectural component:
 - a list of loss sensitive data of impact class [IMP.AVAL.LOSS.Medium] or higher persistently stored at the architectural component;
 - for each loss sensitive data of impact class [IMP.AVAL.LOSS.Medium] or higher persistently stored at the architectural component:
 - a description of corresponding automatic data transfer mechanism including possible transfer destinations.

The following test setups shall be prepared:

- for each architectural component, a test setup based on a sample internet connected toy in default configuration for identifying:
 - loss sensitive data persistently stored at the architectural component; and
- for each documented automatic data transfer mechanism, a test setup to generate and automatically receive loss sensitive data.

Assessment activities:

- The internet connected toy's conformity to [BACKUP-AUTOTRANS] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by:
 - an inspection of the internet connected toy's physical human interfaces for persistently stored loss sensitive data of impact class [IMP.AVAL.LOSS.Medium] or higher;
 - a scan of the internet connected toy's logical interfaces for persistently stored loss sensitive data of impact class [IMP.AVAL.LOSS.Medium] or higher.

- For each documented automatic data transfer mechanism, its correct implementation shall be verified generating and automatically receiving loss sensitive data.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [BACKUP-AUTOTRANS]; and
- the verification of the correctness and completeness of the documentation was successful; and
- the verification of the correct implementation of each documented automatic data transfer mechanism was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correctness and completeness of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each automatic data transfer mechanism.

6.2.6 Assessment criteria for [BACKUP-EXPORT]

Assessment reference:

[\[BACKUP-EXPORT\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [BACKUP-EXPORT];
- a functional completeness assessment on the internet connected toy capabilities that are addressed by [BACKUP-EXPORT];
- a functional sufficiency assessment of each data export mechanisms used by the internet connected toy to fulfil [BACKUP-EXPORT];

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of internet connected toy's architectural components;
- for each architectural component:
 - a list of loss sensitive data of impact class [IMP.AVAI.LOSS.Medium] or higher persistently stored at the architectural component;
 - for each loss sensitive data of impact class [IMP.AVAI.LOSS.Medium] or higher persistently stored at the architectural component:
 - a description of corresponding data export mechanisms including possible transfer destinations.

The following test setups shall be prepared:

- for each architectural component, a test setup based on a sample internet connected toy in default configuration for identifying:
 - loss sensitive data persistently stored at the architectural component; and
- for each architectural component, a test setup to export and automatically receive all loss sensitive data of impact class [IMP.AVAI.LOSS.Medium] or higher persistently stored at the architectural component.

Assessment activities:

- The internet connected toy's conformity to [BACKUP-EXPORT] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by:
 - an inspection of the internet connected toy's physical human interfaces for persistently stored loss sensitive data of impact class [IMP.AVAI.LOSS.Medium] or higher;
 - a scan of the internet connected toy's logical interfaces for persistently stored loss sensitive data of impact class [IMP.AVAI.LOSS.Medium] or higher.
- For each architectural component, the correct implementation of the data export mechanisms shall be verified by exporting and receiving all loss sensitive data of impact class [IMP.AVAI.LOSS.Medium] or higher persistently stored at the architectural component.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [BACKUP-EXPORT]; and
- the verification of the correctness and completeness of the documentation was successful; and
- the verification of the correct implementation of each documented data export mechanism was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correctness and completeness of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each data export mechanism.

6.3 No known exploitable vulnerabilities

6.3.1 Assessment criteria for [NKEV-MKAV]

Assessment reference:

[\[NKEV-MKAV\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [NKEV-MKAV], where potential known exploitable vulnerabilities are identified either:
 - based on an SBOM; or
 - based on a vulnerability scanner applied to the default configuration of the internet connected toy required by clause [5.4](#).
- (if the assessment is based on a vulnerability scanner) a functional completeness assessment of the identified known exploitable vulnerabilities beneath the documented remediation plan.

Assessment preparation:

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

- a remediation plan for known exploitable vulnerabilities;
- (if the assessment is based on an SBOM and the SBOM is transitive) the SBOM of the internet connected toy.

(If the assessment is based on a vulnerability scanner) The following test setups shall be prepared:

- the internet connected toy shall be set up in default configuration;
- a vulnerability scanner for the internet connected toy shall be set up.

Assessment activities:

- A list of potential vulnerabilities shall be created either by:
 - (if the assessment is based on an SBOM and the SBOM is transitive) consulting <https://euvd.enisa.europa.eu/> based on the internet connected toy's details including the transitive SBOM and analysing the results for known exploitable vulnerabilities;
 - (if the assessment is based on a vulnerability scanner) applying the vulnerability scanner on the internet connected toy and analysing the results for known exploitable vulnerabilities.
- The internet connected toy's conformity to [NKEV-MKAV] shall be validated based on the documentation by:
 - verifying that the remediation plan covers all known exploitable vulnerabilities.

Assessment verdict:

The verdict PASS shall be assigned when:

- no known exploitable vulnerabilities are found or
- only known exploitable vulnerabilities are found which are covered and processed according to the remediation plan.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the identified potential vulnerabilities and their analysis for known exploitable vulnerabilities;
- records of the validation of the documentation.

6.3.2 Assessment criteria for [NKEV-INIT-UDP]

Assessment reference:

[\[NKEV-INIT-UDP\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [NKEV-INIT-UDP];
- a functional sufficiency assessment the internet connected toy's behaviour on first start or after factory reset to fulfil [NKEV-INIT-UDP];

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- For each architectural component:
 - documentation describing the behaviour on first start or first start after factory reset; including
 - software update mechanisms used to request information on the availability of security update packages or request and install available security update packages;
 - interfaces and network connections used by the software update mechanisms;
 - notification mechanisms to notify guardians when security update packages are available;
 - interfaces and network connections used by the software update mechanisms.

The following test setups shall be prepared:

- internet connected toy in its default configuration;
- documented interfaces and network connections used by software update mechanisms or notification mechanisms.

Assessment activities:

- The internet connected toy's conformity to [NKEV-INIT-UDP] shall be validated based on the documentation.
- For each architectural component on first start or first start after factory reset:
 - verify whether information on the availability of security update packages are requested;
 - verify whether guardians are notified when security update packages are available;
 - if not blocked by the entity that puts the architectural component into first use:
 - verify whether available security update packages are requested and installed.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity with [NKEV-INIT-UDP]; and
- All architectural component on first start or first start after factory reset:
 - information on the availability of security update packages are requested; and
 - guardians are notified when security update packages are available; and
 - where not blocked by the entity that puts the architectural component into first use:
 - available security update packages are requested and installed.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests.

6.4 Secure by default configuration

6.4.1 Assessment criteria for [SDC-AUM-FH]

Assessment reference:

[\[SDC-AUM-FH\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [SDC-AUM-FH];
- a functional completeness assessment on the internet connected toy's capabilities that are addressed by [SDC-AUM-FH];

based on the factory default state.

NOTE 1: A functional sufficiency assessment of each authentication mechanism used by the internet connected toy to fulfil [SDC-AUM-FH] is addressed by the assessment of [AUM-FH].

Assessment preparation:

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

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

NOTE 2: This documentation is a subset of the documentation required for the assessment of [AUM-FH]

The following test setups shall be prepared:

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

Assessment activities:

- The internet connected toy's conformity to [SDC-AUM-FH] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by:
 - inspecting the internet connected toy in factory default state; and
 - (if functions whose use can cause harm can be configured during initialisation) performing the initialisation without providing explicit confirmation of configurations deviating from the minimal required authentication strength determined by table 2 and inspecting the internet connected toy after initialisation.

Assessment verdict:

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

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

6.4.2 Assessment criteria for [SDC-SUM-AUTO]

Assessment reference:

[\[SDC-SUM-AUTO\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [SDC-SUM-AUTO];
- a functional sufficiency assessment of each software update mechanism used by the internet connected toy to fulfil [SDC-SUM-AUTO];

based on the factory default state.

Assessment preparation:

The following documentation for the internet connected toy's shall be complete for each architectural component:

- documentation describing all supported software update mechanism that support automated security updates, where automated security updates are used in the factory default state or whose use can be activated during initialisation;
- documentation describing updatable parts of the internet connected toy's software where automated security updates are not used in the factory default state or activation is not supported during initialisation;
- (if the internet connected toy does not use automated security updates in the factory default state or activation of use is not supported during initialisation for an updatable part of its software):
 - a justified statement that each of the internet connected toy's architectural component has no capability to connect to public networks; or
 - for each updatable part of the internet connected toy's software that does not use automated security updates in the factory default state or activation is not supported during initialisation an explanation of why automatic installation of updates would create an unacceptable risk to essential function availability or safety; or
 - a list of time sensitive function with IMP.AVAL.TIME.High that is provided by the architectural component.

NOTE: This documentation is mostly a subset of the documentation required for the assessment of [SU-AUTO].

The following test setups shall be prepared:

- for each software update mechanism where automated security updates are used in the factory default state or whose use can be activated during initialisation:
 - a test setup that allows to perform a corresponding automated security update.

Assessment activities:

- The internet connected toy's conformity to [SDC-SUM-AUTO] shall be validated based on the documentation.
- For each software update mechanism where automated security updates are used in the factory default state or whose use can be activated during initialisation, its correct implementation shall be verified by:
 - initialising the internet connected toy without changes to the preconfigured settings; and
 - providing a corresponding software package in a form that triggers the automated security update;
 - checking whether the internet connected toy performs the automated security update; and
 - confirming whether the software version has been updated to a new version.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [SDC-SUM-AUTO]; and
- the verification of the correct implementation of the use of each software update mechanism was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of the use of each software update mechanism where automated security updates are used in the factory default state or whose use can be activated during initialisation.

6.4.3 Assessment criteria for [SDC-SUM-NOTIF]

Assessment reference:

[\[SDC-SUM-NOTIF\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [SDC-SUM-NOTIF];
- a functional completeness assessment on the internet connected toy capabilities that are addressed by [SDC-SUM-NOTIF];

based on the factory default state.

Assessment preparation:

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

- documentation describing all supported software update notification mechanisms where software update notification are used in the factory default state or whose use can be activated during initialisation, including:
 - a description of how software update notifications are triggered; and
 - a description of how notifications are received, and

- documentation describing parts of the internet connected toy's updatable software where software update notification is not used in the factory default state or whose use can not be activated during initialisation, including:
 - (if the internet connected toy does not use software update notification in the factory default state or whose use can not be activated during initialisation for an updatable part of its software):
 - a justified statement that each of the internet connected toy's architectural component has no capability to connect to public networks.

NOTE: This documentation is a subset of the documentation required for the assessment of [SU-NOTIF].

The following test setups shall be prepared:

- for each software update notification mechanism where software update notification is used in the factory default state or whose use can be activated during initialisation:
 - a test setup that allows to trigger software update notifications, and
 - a test setup that allows to receive software update notifications based on a sample internet connected toy in default configuration.

Assessment activities:

- The internet connected toy's conformity to [SDC-SUM-AUTO] shall be validated based on the documentation.
- For each software update notification mechanism where software update notification is used in the factory default state or whose use can be activated during initialisation, its correct implementation shall be verified by:
 - initialising the internet connected toy without changes to the preconfigured settings, and
 - triggering a software update notification; and
 - checking whether the software update notification mechanism automatically notifies the internet connected toy's users.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [SDC-SUM-NOTIF]; and
- the verification of the correct implementation of the use of each software update notification mechanism where software update notification is used in the factory default state or whose use can be activated during initialisation was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of the use of software update notification mechanism where software update notification is used in the factory default state or whose use can be activated during initialisation was successful.

6.4.4 Assessment criteria for [SDC-FRM]

Assessment reference:

[\[SDC-FRM\]](#)

Assessment objective:

The assessment functionally determines whether all user-related data, installed applications, and configurations deviating from the default state are erased after using the factory reset mechanism.

Assessment preparation:

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

- documentation on how the factory reset mechanism can be accessed;
- the internet connected toy shall be set up and some configuration changes shall be created and persistently stored;
- where the internet connected toy supports the storage of user-related data, some user-related data shall be created and persistently stored on the internet connected toy;
- where the internet connected toy supports the installation of applications, some common application for the internet connected toy shall be installed.

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

Assessment activities:

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

Assessment verdict:

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

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- description of the performed test;
- all test records of the performed test.

6.4.5 Assessment criteria for [SDC-PARCONT]

Assessment reference:

[\[SDC-PARCONT\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [SDC-PARCONT];
- a functional completeness assessment on the internet connected toy capabilities that are addressed by [SDC-PARCONT];

based on the default configuration required by clause [5.4](#).

NOTE: A functional sufficiency assessment of each parental control function used by the internet connected toy to fulfil [SDC-PARCONT] is addressed by the assessment of [PARCONT].

Assessment preparation:

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

- a list of internet connected toy's functions that are intended to be used by children;

- for each function that is intended to be used by children, a list of corresponding parental control functions including the parental control configuration possibilities concerning:
 - child's access rights on the internet connected toy;
 - sources where children are allowed to access external content from; and
 - persons that are allowed to communicate with children

The following test setups shall be prepared:

- a test setup for identifying functions, corresponding parental control functions and associated parental control configuration possibilities based on a sample internet connected toy in default configuration;
- a test setup for using parental control functions and assessing the enforcement of parental control configuration based on a sample internet connected toy in default configuration.

Assessment activities:

- The internet connected toy's conformity to [SDC-PARCONT] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by:
 - inspecting the internet connected toy in factory default state; and
 - (if parental control functions can be configured during initialisation) performing the initialisation without providing explicit confirmation of configurations after initialisation; and
 - an inspection of the internet connected toy for functions, corresponding parental control functions and associated parental control configuration possibilities that are accessible via human interfaces.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [SDC-PARCONT]; and
- the verification of the correctness and completeness of the documentation was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

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

6.4.6 Assessment criteria for [SDC-MON-HANDLE]

Assessment reference:

[\[SDC-MON-HANDLE\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of each audit event data generated by a monitoring mechanism of the internet connected toy to fulfil [SDC-MON-HANDLE]

based on the default configuration required by clause [5.4](#).

NOTE: Part of the functional sufficiency assessment to fulfil [SDC-AUM-FH] is addressed by the assessment of [MON-HANDLE].

Assessment preparation:

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

- for each architectural component:
 - documentation on support of public communication;
 - list of all audit event data generated by a monitoring mechanism and for each entry:
 - corresponding logging mechanism or data transfer mechanism.

The following test setups shall be prepared:

- for each logging mechanism in *assessment preparation*, a test setup that allows to:
 - generate audit event data;
 - access the storage location where logging data is stored.
- for each data transfer mechanism in *assessment preparation*, a test setup that allows to:
 - generate audit event data;
 - access the architectural component or other device where the data is transferred to.

Assessment activities:

The following activities shall be performed:

- For each audit event data listed in *assessment preparation* with assigned logging mechanism:
 - Generate audit event data; and
 - check that the logging data produced by the logging mechanism from the audit event data is generated and stored.
- For each audit event data listed in *assessment preparation* with assigned data transfer mechanism:
 - Generate audit event data; and
 - check that the audit event data is transferred to the destination (architectural component or other device).

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity with [SDC-MON-HANDLE];
- for every audit event data assigned to a logging mechanism corresponding logging data is generated and stored; and
- for every audit event data assigned to a data transfer mechanism audit event data is transferred to the destination.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

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

6.4.7 Assessment criteria for [CRY-GENERAL]

Compliance with [CRY-GENERAL] shall be assessed according to the assessment criteria provided in annex [K](#).

6.4.8 Assessment criteria for [CRY-CCK-PRE-LEN]

Assessment reference:

[\[CRY-CCK-PRE-LEN\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [CRY-CCK-PRE-LEN].
- a functional completeness assessment on the internet connected toy's preinstalled long term confidential cryptographic keys.

Assessment preparation:

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

- a list of internet connected toy's preinstalled long term confidential cryptographic keys;
- for each preinstalled long term confidential cryptographic key:
 - a description of generation method of the confidential cryptographic key;
 - its key sizes and corresponding security strength including a justification for the security strength.

The following test setups shall be prepared:

- for each architectural component, a test setup for identifying and analysing preinstalled long term confidential cryptographic keys;

Assessment activities:

- The internet connected toy's conformity to [CRY-CCK-PRE-LEN] shall be validated based on the documentation.
- For each architectural component, the correctness and completeness of the documentation shall be verified by:
 - identifying and analysing preinstalled long term confidential cryptographic keys.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [CRY-CCK-PRE-LEN]; and
- the verification of the correctness and completeness of the documentation was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

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

6.4.9 Assessment criteria for [CRY-CCK-GEN]

Assessment reference:

[\[CRY-CCK-GEN\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [CRY-CCK-GEN];
- a functional sufficiency assessment of each long term confidential cryptographic key generation mechanisms used by the internet connected toy to fulfil [CRY-CCK-GEN];

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of internet connected toy's long term confidential cryptographic key generation mechanisms;
- for each long term confidential cryptographic key generation mechanism:
 - a description of the confidential cryptographic key generation mechanism;
 - a list of generated key sizes in default configuration and the corresponding security strength including a justification for the security strength.

The following test setups shall be prepared:

- for each internet connected toy's long term confidential cryptographic key generation mechanism, a test setup for generating and extracting corresponding long term confidential cryptographic keys based on a sample internet connected toy in default configuration.

Assessment activities:

- The internet connected toy's conformity to [CRY-CCK-GEN] shall be validated based on the documentation.
- For each internet connected toy's long term confidential cryptographic keys generation mechanism, its correct implementation shall be verified by generating, extracting and inspecting generated long term confidential cryptographic keys.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [CRY-CCK-GEN]; and
- the verification of the correct implementation of each internet connected toy's long term confidential cryptographic key generation mechanism was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each internet connected toy's long term confidential cryptographic key generation mechanism.

6.4.10 Assessment criteria for [CRY-PW-PRE-COM]

Assessment reference:

[\[CRY-PW-PRE-COM\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [CRY-PW-PRE-COM];
- a functional completeness assessment on the internet connected toy's preinstalled passwords.

Assessment preparation:

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

- a list of internet connected toy's preinstalled passwords;
- for each preinstalled password:
 - a description of generation method of the password;
 - its complexity and the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) for the corresponding authentication mechanisms' usage, including a justification for the password's complexity.

The following test setups shall be prepared:

- for each architectural component, a test setup for identifying and analysing preinstalled passwords;

Assessment activities:

- The internet connected toy's conformity to [CRY-PW-PRE-COM] shall be validated based on the documentation.
- For each architectural component, the correctness and completeness of the documentation shall be verified by:
 - identifying and analysing preinstalled passwords.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [CRY-PW-PRE-COM]; and
- the verification of the correctness and completeness of the documentation was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

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

6.4.11 Assessment criteria for [CRY-PW-GEN-COM]

Assessment reference:

[\[CRY-PW-GEN-COM\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [CRY-PW-GEN-COM];
- a functional sufficiency assessment of each password generation mechanisms used by the internet connected toy to fulfil [CRY-PW-GEN-COM];

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of internet connected toy's password generation mechanisms;
- for each password generation mechanism:
 - a description of the password generation mechanism;
 - a list of generated passwords;
 - for each password its default complexity and the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) for the corresponding authentication mechanisms' usage, including a justification for the password's complexity.

The following test setups shall be prepared:

- for each internet connected toy's password generation mechanism, a test setup for generating and extracting corresponding passwords based on a sample internet connected toy in default configuration.

Assessment activities:

- The internet connected toy's conformity to [CRY-PW-GEN-COM] shall be validated based on the documentation.
- For each internet connected toy's password generation mechanism, its correct implementation shall be verified by generating, extracting and inspecting generated passwords.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [CRY-PW-GEN-COM]; and
- the verification of the correct implementation of each internet connected toy's long term confidential cryptographic keys generation mechanism was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each internet connected toy's password generation mechanism.

6.4.12 Assessment criteria for [CRY-PW-USR-COM]

Assessment reference:

[\[CRY-PW-USR-COM\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [CRY-PW-USR-COM];
- a functional completeness assessment of each option for users to choose passwords;
- a functional sufficiency assessment of each option for users to choose passwords;

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of internet connected toy's options for users to choose passwords;
- for each option for the user to choose passwords:
 - the password's default complexity and the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) for the corresponding authentication mechanisms' usage, including a justification for the password's complexity;
 - a statement whether users can choose passwords deviating from the the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$);
 - (where users can choose passwords deviating from the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$)), a description of how the warning is performed and explicit user consent is obtained.

The following test setups shall be prepared:

- for each option for users to choose passwords, a test setup for setting and extracting corresponding passwords based on a sample internet connected toy in default configuration;
- for each architectural component, a test setup for identifying and analysing options for users to choose passwords.

Assessment activities:

- The internet connected toy's conformity to [CRY-PW-USR-COM] shall be validated based on the documentation.
- For each architectural component, the correctness and completeness of the documentation shall be verified by:
 - identifying options for users to choose passwords.
- For each options for users to choose passwords, its correct implementation shall be verified by:
 - trying to choose passwords deviating from the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$).

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [CRY-PW-USR-COM]; and
- the verification of the correctness and completeness of the documentation was successful; and
- the verification of the correct implementation of each option for users to choose passwords was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correctness and completeness of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of option for users to choose passwords.

6.5 Security updates

6.5.1 Assessment criteria for [SU-SUPPORT]

Assessment reference:

[\[SU-SUPPORT\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [SU-SUPPORT];
- a functional completeness assessment on the internet connected toy's capabilities that are addressed by [SU-SUPPORT];
- a functional sufficiency assessment of each software update mechanism used by the internet connected toy to fulfil [SU-SUPPORT];

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of all architectural components of the internet connected toy;
- for each architectural component:
 - a list of its software including a declaration of immutability;
 - for each software that are declared immutable, a technical description on the corresponding measures including a justification for the immutable design;
 - documentation describing all supported software update mechanisms, including:
 - their scope; and
 - interfaces through which updates can be invoked.

The following test setups shall be prepared:

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

Assessment activities:

- The internet connected toy's conformity to [SU-SUPPORT] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by:
 - inspecting the internet connected toy to identify software architectural components.
- For each software update mechanism, its correct implementation shall be verified by:
 - installing an update over this software update mechanism to update a software architectural component; and
 - checking whether the software has changed to the updated software.

Assessment verdict:

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correctness and completeness of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each software update mechanism.

6.5.2 Assessment criteria for [SU-PROVIDE]

Assessment reference:

[\[SU-PROVIDE\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [SU-PROVIDE];
- a functional completeness assessment on the capabilities of the internet connected toy's architectural components that are addressed by [SU-PROVIDE];
- a functional sufficiency assessment of each software update mechanism provided by the internet connected toy's architectural components to fulfil [SU-PROVIDE];

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

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

The following test setups shall be prepared:

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

Assessment activities:

- The internet connected toy's conformity to [SU-PROVIDE] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by:
 - inspecting the architectural components of the internet connected toy that include core software and
 - checking whether each identified component is associated with a documented update path.
- For each software update mechanism, its correct implementation shall be verified by:
 - installing an update over this software update mechanism to update a software architectural component; and
 - checking whether the software has changed to the updated software.

Assessment verdict:

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correctness and completeness of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each software update mechanism.

6.5.3 Assessment criteria for [SU-AUTO]

Assessment reference:

[\[SU-AUTO\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [SU-AUTO];
- a functional sufficiency assessment of each software update mechanism used by the internet connected toy to fulfil [SU-AUTO];

based on explicit configuration of software update mechanism to use automated security update.

Assessment preparation:

The following documentation for the internet connected toy shall be complete for each architectural component:

- documentation describing all supported software update mechanism, including:
 - the parts of the internet connected toy's software that can be updated by the software update mechanism;
 - the interfaces through which updates can be invoked;
 - their capability to perform automated security updates.

- documentation describing updatable parts of the internet connected toy's software that do not support automated security updates;
- (if the internet connected toy does not support automated security updates for an updatable part of its software):
 - a justified statement that each of the internet connected toy's architectural component has no capability to connect to public networks; or
 - for each updatable part of the internet connected toy's software that does not support automated security updates an explanation of why automatic installation of updates would create an unacceptable risk to essential function availability or safety.

The following test setups shall be prepared:

- for each software update mechanism that supports automated security updates, a test setup that allows to perform a corresponding automated security update.

Assessment activities:

- The internet connected toy's conformity to [SU-AUTO] shall be validated based on the documentation.
- For each software update mechanism that supports automated security updates, its correct implementation shall be verified by:
 - providing a corresponding software package in a form that triggers the automated security update;
 - checking whether the product performs the automated security update; and
 - confirming whether the software version has been updated to a new version.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity with [SU-AUTO]; and
- the verification of the correct implementation of each software update mechanism was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each software update mechanism that supports automated security updates.

6.5.4 Assessment criteria for [SU-DISABLE-AUTO]

Assessment reference:

[\[SU-DISABLE-AUTO\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [SU-DISABLE-AUTO];
- a functional sufficiency assessment of each software update mechanism that support automated security updates used by the internet connected toy to fulfil [SU-DISABLE-AUTO];

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- list of all software update mechanism that support automated security updates;
 - documentation on how to disable these software update mechanisms;
- documentation on entities intended to operate the internet connected toy.

The following test setups shall be prepared:

- for each software update mechanism that supports automated security updates, a test setup that allows to perform a corresponding automated security update.

Assessment activities:

The following activities shall be performed:

- The internet connected toy's conformity to [SU-DISABLE-AUTO] shall be validated based on the documentation.
- For each software update mechanism that supports automated security updates, its correct disable mechanisms implementation shall be verified by:
 - disabling the software update mechanism as documented;
 - providing a corresponding software package in a form that triggers the automated security update;
 - checking that the product does not perform the automated security update.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity with [SU-DISABLE-AUTO]; and
- the verification of the correct implementation of each software update mechanism disable mechanism was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each software update mechanism disable mechanism.

6.5.5 Assessment criteria for [SU-POSTPONE-AUTO]

Assessment reference:

[\[SU-POSTPONE-AUTO\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [SU-POSTPONE-AUTO];
- a functional sufficiency assessment of each software update mechanism that support automated security updates used by the internet connected toy to fulfil [SU-POSTPONE-AUTO];

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- list of all software update mechanism that support automated security updates;
- documentation on how to postpone automated updates;
- documentation on entities intended to operate the internet connected toy.

The following test setups shall be prepared:

- for each software update mechanism that supports automated security updates, a test setup that allows to perform a corresponding automated security update.

Assessment activities:

- The internet connected toy's conformity to [SU-POSTPONE-AUTO] shall be validated based on the documentation.
- For each software update mechanism that supports automated security updates, its correct postpone mechanisms implementation shall be verified by:
 - postpone the automated installation of updates as documented for a fixed time;
 - providing a corresponding software package in a form that triggers the automated security update;
 - checking that the product does not perform the automated security update during the fixed postpone-time; and
 - checking that the product performs the automated security update after the fixed postpone-time.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity with [SU-POSTPONE-AUTO]; and
- the verification of the correct implementation of the mechanism to temporary postpone the automated installation of updates was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of the mechanism to temporary postpone the automated installation of updates.

6.5.6 Assessment criteria for [SU-NOTIF]

Assessment reference:

[\[SU-NOTIF\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [SU-NOTIF];
- a functional sufficiency assessment of each software update notification mechanism used by the internet connected toy to fulfil [SU-NOTIF];

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- documentation describing all supported software update notification mechanisms, including:
 - a description of how software update notifications are triggered; and
 - a description of how notifications are received; and
- documentation describing parts of the internet connected toy's updatable software where software update notification is not supported:
 - (if the internet connected toy does not support software update notification for an updatable part of its software);
 - a justified statement that each of the internet connected toy's architectural component has no capability to connect to public networks.

The following test setups shall be prepared:

- for each software update notification mechanism:
 - a test setup that allows to trigger update notifications; and
 - a test setup that allows to receive update notifications based on a sample internet connected toy in default configuration.

Assessment activities:

- The internet connected toy's conformity to [SU-NOTIF] shall be validated based on the documentation.
- For each software update notification mechanism, its correct implementation shall be verified by:
 - triggering a software update notification; and
 - checking whether the software update notification mechanism automatically notifies the internet connected toy's users that an update of its software is available.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity with [SU-NOTIF]; and
- the verification of the correct implementation of each software update notification mechanism was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each software update notification mechanism.

6.6 Authentication and access control

6.6.1 Assessment criteria for [ACM-FH]

Assessment reference:

[\[ACM-FH\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [ACM-FH];
- a functional completeness assessment on the internet connected toy capabilities that are addressed by [ACM-FH];
- a functional sufficiency assessment of each access control mechanism used by the internet connected toy to fulfil [ACM-FH];

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of internet connected toy's functions whose use can cause harm;
- for each function, whose use can cause harm:
 - its impact class IMP.FH;
 - the physical operational environment of the architectural component that performs the function;
 - for each of the function's trigger input possibilities:
 - the interface and communication type;
 - a list of corresponding access control mechanisms including their default authorisation policy.

The following test setups shall be prepared:

- a test setup for identifying functions, their trigger input possibilities and corresponding access control mechanisms based on a sample internet connected toy in default configuration;
- for each access control mechanism, a test setup that allows privilege escalation attacks from authenticated entities and unauthorised access attempts of unauthenticated entities.

Assessment activities:

- The internet connected toy's conformity to [ACM-FH] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by:
 - an inspection of the internet connected toy for functions and related access control mechanisms that are accessible via physical human interfaces;
 - a scan of the internet connected toy for functions and related access control mechanisms that are accessible via logical interfaces.
- For each access control mechanism, its correct implementation shall be verified based on attempts to violate the authorisation policy by:
 - privilege escalation of authenticated entities based on the default authorisation policy;
 - unauthorised usage of function, whose use can cause harm by unauthenticated entities based on the default authorisation policy.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [ACM-FH]; and
- the verification of the correctness and completeness of the documentation was successful; and

- the verification of the correct implementation of each access control mechanism was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correctness and completeness of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each access control mechanism.

6.6.2 Assessment criteria for [PARCONT]

Assessment reference:

[\[PARCONT\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [PARCONT];
- a functional completeness assessment on the internet connected toy capabilities that are addressed by [PARCONT];
- a functional sufficiency assessment of each parental control function used by the internet connected toy to fulfil [PARCONT];

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of internet connected toy's functions that are intended to be used by children;
- for each function that is intended to be used by children, a list of corresponding parental control functions including the parental control configuration possibilities concerning:
 - child's access rights on the internet connected toy;
 - sources where children are allowed to access external content from; and
 - persons that are allowed to communicate with children.

The following test setups shall be prepared:

- a test setup for identifying functions, corresponding parental control functions and associated parental control configuration possibilities based on a sample internet connected toy in default configuration;
- a test setup for using parental control functions and assessing the enforcement of parental control configuration based on a sample internet connected toy in default configuration.

Assessment activities:

- The internet connected toy's conformity to [PARCONT] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by:
 - an inspection of the internet connected toy for functions, corresponding parental control functions and associated parental control configuration possibilities that are accessible via human interfaces;

- For each function that is intended to be used by children, its correct implementation of corresponding parental control functions and associated parental control configuration possibilities shall be verified by:
 - performing changes to the parental control configuration via the corresponding parental control functions'; and
 - assessing the enforcement of the parental control configuration changes from a child's perspective.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [PARCONT]; and
- the verification of the correctness and completeness of the documentation was successful; and
- for each function that is intended to be used by children the verification of the correct implementation of parental control functions was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correctness and completeness of the documentation;
- descriptions of the performed tests and documentation of associated test records that verify the correct implementation of the parental control functions.

6.6.3 Assessment criteria for [AUM-FH]

Assessment reference:

[\[AUM-FH\]](#)

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of internet connected toy's functions whose use can cause harm;
- for each function, whose use can cause harm:
 - its impact class IMP.FH;
 - the physical operational environment of the architectural component that performs the function;
 - for each of the function's trigger input possibilities:
 - the interface and communication type;

- a list of corresponding authentication mechanisms including:
 - the authentication mechanisms' strength;
 - the type of authentication factors;
 - the documentation defined in the corresponding assessments in clause [E.1.2](#) in Assessment preparation.

The following test setups shall be prepared:

- a test setup for identifying functions, their trigger input possibilities and corresponding authentication mechanisms based on a sample internet connected toy in default configuration;
- 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.

Assessment activities:

- The internet connected toy's conformity to [AUM-FH] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by:
 - an inspection of the internet connected toy for functions and related authentication mechanisms that are accessible via physical human interfaces;
 - a scan of the internet connected toy for functions and related authentication mechanisms that are accessible via logical interfaces.
- 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.

Assessment verdict:

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correctness and completeness of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each authentication mechanism.

6.6.4 Assessment criteria for [AUTHZ-LP]

Assessment reference:

[\[AUTHZ-LP\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [AUTHZ-LP].

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

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

Assessment activities:

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

Assessment verdict:

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation.

6.6.5 Assessment criteria for [AUTHZ-R]

Assessment reference:

[\[AUTHZ-R\]](#)

Assessment objective:

The assessment covers:

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

Assessment preparation:

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

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

The following test setups shall be prepared:

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

Assessment activities:

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

Assessment verdict:

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

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

6.6.6 Assessment criteria for [AUTHZ-PC]

Assessment reference:

[\[AUTHZ-PC\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of the internet connected toy's authorisation policy to fulfil [AUTHZ-PC]

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of the internet connected toy's parental control functions.

The following test setups shall be prepared:

- a test setup for using parental control functions and assessing the enforcement of parental control configuration based on a sample internet connected toy in default configuration.

Assessment activities:

- For each parental control function, the correct implementation of the corresponding authorisation policy shall be verified by:
 - attempting to use parental control function from the perspective of an child; and
 - assessing the effects of the usage attempts on the enforcement of parental control configuration.

Assessment verdict:

The verdict PASS shall be assigned if:

- for each parental control function, the correct implementation of the authorisation policy was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- descriptions of the performed tests and records of performed tests to verify the correct implementation of parental control function's authorisation policy.

6.7 Confidentiality protection

6.7.1 Assessment criteria for [CONF-SSM]

Assessment reference:

[\[CONF-SSM\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [CONF-SSM];
- a functional completeness assessment on the internet connected toy capabilities that are addressed by [CONF-SSM];
- a functional sufficiency assessment of each confidentiality protecting secure storage mechanism used by the internet connected toy to fulfil [CONF-SSM],

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of internet connected toy's confidential data that are intended to be persistently stored by the internet connected toy;
- for each confidential data that are intended to be persistently stored by the internet connected toy:
 - its impact class IMP.CONF;
 - a list of architectural components that store the confidential data including:
 - its physical operational environment;
 - a list of storage locations for the confidential data;
 - a list of corresponding confidentiality protecting secure storage mechanisms including their strengths.

The following test setups shall be prepared:

- for each architectural component, a test setup for identifying confidential data, their storage location and corresponding confidentiality protecting secure storage mechanisms based on a sample internet connected toy in default configuration;
- for each confidentiality protecting secure storage mechanism, a test setup defined by the test cases provided in clause [E.3](#) according to the needs determined by its strength.

Assessment activities:

- The internet connected toy's conformity to [CONF-SSM] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by:
 - an inspection of the internet connected toy's physical human interfaces for persistently storable/stored confidential data, related storage locations and confidentiality protecting secure storage mechanisms;
 - a scan of the internet connected toy's logical interfaces for persistently storable/stored confidential data, related storage locations and confidentiality protecting secure storage mechanisms.
- For each confidentiality protecting secure storage mechanism, its correct implementation shall be verified based on the test cases provided in clause [E.3](#) according to the needs determined by its strength.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [CONF-SSM]; and
- the verification of the correctness and completeness of the documentation was successful; and

- the verification of the correct implementation of each confidentiality protecting secure storage mechanism was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correctness and completeness of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each confidentiality protecting secure storage mechanism

6.7.2 Assessment criteria for [CONF-COM]

Assessment reference:

[\[CONF-COM\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [CONF-COM];
- a functional completeness assessment on the internet connected toy capabilities that are addressed by [CONF-COM];
- a functional sufficiency assessment of each confidentiality protecting communication mechanism used by the internet connected toy to fulfil [CONF-COM]

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of internet connected toy's confidential data that are intended to be communicated by or to the internet connected toy;
- for each confidential data that are intended to be communicated by or to the internet connected toy:
 - its impact class IMP.CONF;
 - a list of architectural components that can communicate the confidential data including:
 - its physical operational environment
 - the corresponding interfaces and communication types;
 - a list of corresponding confidentiality protecting communication mechanisms including their strengths.

The following test setups shall be prepared:

- for each architectural component, a test setup based on a sample internet connected toy in default configuration for identifying:
 - confidential data that can be communicated by or to the architectural component;
 - the corresponding interfaces and communication types for communication;
 - the corresponding confidentiality protecting communication mechanisms;

- for each confidentiality protecting communication mechanism, a test setup defined by the test cases provided in clause [E.3](#) according to the needs determined by its strength.

Assessment activities:

- The internet connected toy's conformity to [CONF-COM] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by:
 - an inspection of the internet connected toy's physical human interfaces for communicable confidential data, related communication capabilities and confidentiality protecting communication mechanisms;
 - a scan of the internet connected toy's logical interfaces for communicable confidential data, related communication capabilities and confidentiality protecting communication mechanisms.
- For each confidentiality protecting communication mechanism, its correct implementation shall be verified based on the test cases provided in clause [E.3](#) according to the needs determined by its strength.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [CONF-COM]; and
- the verification of the correctness and completeness of the documentation was successful; and
- the verification of the correct implementation of each confidentiality protecting communication mechanism was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correctness and completeness of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each confidentiality protecting communication mechanism

6.8 Integrity protection

6.8.1 Assessment criteria for [INT-SSM]

Assessment reference:

[\[INT-SSM\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [INT-SSM];
- a functional completeness assessment on the internet connected toy capabilities that are addressed by [INT-SSM];
- a functional sufficiency assessment of each integrity protecting secure storage mechanism used by the internet connected toy to fulfil [INT-SSM]

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of internet connected toy's integrity relevant data that are intended to be persistently stored by the internet connected toy;
- for each integrity relevant data that are intended to be persistently stored by the internet connected toy:
 - its impact class IMP.INT;
 - a list of architectural components that store the integrity relevant data including:
 - its physical operational environment;
 - a list of storage locations for the integrity relevant data;
 - a list of corresponding integrity protecting secure storage mechanisms including their strengths.

The following test setups shall be prepared:

- for each architectural component, a test setup for identifying integrity relevant data, their storage location and corresponding integrity protecting secure storage mechanisms based on a sample internet connected toy in default configuration;
- for each integrity protecting secure storage mechanism, a test setup defined by the test cases provided in clause [E.2](#) according to the needs determined by its strength.

Assessment activities:

- The internet connected toy's conformity to [INT-SSM] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by:
 - an inspection of the internet connected toy's physical human interfaces for persistently storable/stored integrity relevant data, related storage locations and integrity protecting secure storage mechanisms;
 - a scan of the internet connected toy's logical interfaces for persistently storable/stored integrity relevant data, related storage locations and integrity protecting secure storage mechanisms.
- For each integrity protecting secure storage mechanism, its correct implementation shall be verified based on the test cases provided in clause [E.2](#) according to the needs determined by its strength.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [INT-SSM]; and
- the verification of the correctness and completeness of the documentation was successful; and
- the verification of the correct implementation of each integrity protecting secure storage mechanism was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correctness and completeness of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each integrity protecting secure storage mechanism.

6.8.2 Assessment criteria for [INT-COM]

Assessment reference:

[\[INT-COM\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [INT-COM];
- a functional completeness assessment on the internet connected toy capabilities that are addressed by [INT-COM];
- a functional sufficiency assessment of each integrity protecting communication mechanism used by the internet connected toy to fulfil [INT-COM];

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of internet connected toy's integrity relevant data that are intended to be communicated by or to the internet connected toy;
- for each integrity relevant data that are intended to be communicated by or to the internet connected toy:
 - its impact class IMP.CONF;
 - a list of architectural components that can communicate the integrity relevant data including:
 - its physical operational environment
 - the corresponding interfaces and communication types;
 - a list of corresponding integrity protecting communication mechanisms including their strengths.

The following test setups shall be prepared:

- for each architectural component, a test setup based on a sample internet connected toy in default configuration for identifying:
 - integrity relevant data that can be communicated by or to the architectural component;
 - the corresponding interfaces and communication types for communication;
 - the corresponding integrity protecting communication mechanisms;
- for each integrity protecting communication mechanism, a test setup defined by the test cases provided in clause [E.2](#) according to the needs determined by its strength.

Assessment activities:

- The internet connected toy's conformity to [INT-COM] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by:
 - an inspection of the internet connected toy's physical human interfaces for communicable integrity relevant data, related communication capabilities and integrity protecting communication mechanisms;
 - a scan of the internet connected toy's logical interfaces for communicable integrity relevant data, related communication capabilities and integrity protecting communication mechanisms.
- For each integrity protecting communication mechanism, its correct implementation shall be verified based on the test cases provided in clause [E.2](#) according to the needs determined by its strength.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [INT-COM]; and
- the verification of the correctness and completeness of the documentation was successful; and
- the verification of the correct implementation of each integrity protecting communication mechanism was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correctness and completeness of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each integrity protecting communication mechanism.

6.8.3 Assessment criteria for [INT-SWPCK]

Assessment reference:

[\[INT-SWPCK\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [INT-SWPCK];
- a functional completeness assessment on the internet connected toy capabilities that are addressed by [INT-SWPCK];
- a functional sufficiency assessment of each software package verification mechanism used by the internet connected toy to fulfil [INT-SWPCK];

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of the internet connected toy's architectural components.
- for each architectural component:
 - a list of mechanisms to install software packages;
 - for each internet connected toy's mechanism to install software packages:
 - the communication types of over which software packages can be received
 - a list of software that can be installed by the mechanism including the maximum impact class IMP.INT of corresponding software packages;
 - a list of corresponding software package verification mechanisms including their strengths.

The following test setups shall be prepared:

- for each architectural component, a test setup for identifying mechanisms to install software packages, corresponding software that can be installed, communication types of over which corresponding software packages can be received and corresponding software package verification mechanisms based on a sample internet connected toy in default configuration;
- for each mechanism to install software packages, a test setup defined by the test cases provided in clause [E.2](#) according to the needs determined by its strength.

Assessment activities:

- The internet connected toy's conformity to [INT-SWPCK] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by:
 - an inspection of the internet connected toy's physical human interfaces for mechanism to install software packages;
 - a scan of the internet connected toy's logical interfaces for mechanism to install software packages;
 - for each mechanism to install software packages, performing the installation of a software package to identify software package verification mechanisms.
- For each software package verification mechanism, its correct implementation shall be verified based on the test cases provided in clause [E.2](#) according to the needs determined by its strength.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [INT-SWPCK]; and
- the verification of the correctness and completeness of the documentation was successful; and
- the verification of the correct implementation of each software package verification mechanism was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correctness and completeness of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each software package verification mechanism

6.9 Data minimisation

6.9.1 Assessment criteria for [DMIN-DJST]

Assessment reference:

[\[DMIN-DJST\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of Minimise processed data

Assessment preparation:

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

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

Assessment activities:

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

Assessment verdict:

The verdict PASS shall be assigned if:

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

Otherwise, the verdict FAIL shall be assigned.

Assessment evidence:

- records of the validation of the documentation;

6.10 Availability protection

6.10.1 Assessment criteria for [AVAI-TIME-RECO-POW]

Assessment reference:

[\[AVAI-TIME-RECO-POW\]](#)

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of all internet connected toy's hardware architectural components:
- for each internet connected toy's hardware architectural component:
 - a list of all power supplies
 - for each power supply:
 - a description whether the power supply can power the hardware architectural component alone
 - a list of all functionalities of the internet connected toy that need communication involving the hardware architectural component:
 - for each of these functionalities:
 - a list of interfaces of the internet connected toy, where the operational status of the hardware architectural components can be read including a description on how the operational status can be implied from the interface readings; and

- a list of interfaces of the internet connected toy, where the connection status of the necessary communication channels can be read; or
- parameters of the necessary communication channels of the hardware architectural components in order to externally observe if the connection is active.

The following test setups shall be prepared:

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

Assessment activities:

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

- for every possible order in which the hardware architectural component power supplies can be disconnected or disabled:
 - disconnect or disable all power supplies of the hardware architectural component
 - wait at least 30 s
 - reconnect or enable the power supplies
 - monitor the operational status of the internet connected toy
 - monitor the connection status for all necessary communication channels of the hardware architectural component
 - record the order in which the power supplies are disconnect or disable and reconnect or enable
 - record the time relative to the reconnection or enabling of the last power supply, after which the internet connected toy indicates, that it is operational and all necessary communication channels are established; or
 - record the time relative to the reconnection or enabling of the last power supply, after which every necessary communication channel of the hardware architectural component was active at least once, and there is no indication that the internet connected toy has not resumed operation

Assessment verdict:

The verdict PASS shall be assigned if:

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

Assessment evidence:

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

6.10.2 Assessment criteria for [AVAI-TIME-NETW]**Assessment reference:**

[\[AVAI-TIME-NETW\]](#)

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of all time sensitive function of the internet connected toy:
- for each time sensitive function:
 - description of the functionalities realised or supported by this function
 - list of interfaces necessary for the operation of this function
 - for each interface:
 - communication types of the interface
- a list of interfaces of the internet connected toy, where the status of the architectural component's time sensitive function can be read including a description how the status can be implied from the interface readings.

The following test setups shall be prepared:

- the internet connected toy is set up in default configuration; and
- a test setup to:
 - disconnect or disable the public communication of the internet connected toy's architectural components
 - disconnect or disable the adjacent communication of the internet connected toy's architectural components
 - enable access to at least one interfaces of the internet connected toy, where the status of the internet connected toy's time sensitive function can be read

Assessment activities:

The following activities shall be performed:

- verify the correctness and completeness of the documentation;

- repeat the following steps for communication types public communication, adjacent communication and both, depending on the communication type needed by the functions to be tested:
 - disconnect or disable the corresponding communication type of the internet connected toys architectural component;
 - wait at least 30 s;
 - for each time sensitive function which does not need any interface with the corresponding communication type for its operation:
 - check whether the function is in operable status and record the status of the function and the disconnected or disabled communication type; and
 - reconnect or enable the corresponding communication type.

Assessment verdict:

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

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

6.10.3 Assessment criteria for [AVAI-TIME-RECO-NETW]

Assessment reference:

[\[AVAI-TIME-RECO-NETW\]](#)

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of all functions of the internet connected toy that need communication involving the architectural component:
 - for each of these functions:
 - list of interfaces involving the architectural component and are necessary for the operation of this function:
 - for each interface:
 - communication types of the interface.

- a list of interfaces of the internet connected toy, where the connection status of the necessary communication channels can be read; or
- parameters of the necessary communication channel of the architectural component in order to externally observe if the connection is active.

The following test setups shall be prepared:

- the internet connected toy is set up in default configuration;
- a test setup to:
 - disconnect or disable the public communication of the internet connected toys architectural component;
 - disconnect or disable the adjacent communication of the internet connected toys architectural component;
 - enable access to at least one interfaces of the internet connected toy, where the connection status the necessary interfaces involving the architectural component and are necessary for the operation of these functions can be read; or
 - if the connection status for all necessary interfaces involving the architectural component and are necessary for the operation of these functions cannot be read from the internet connected toy:
 - monitor whether all necessary interfaces involving the architectural component and are necessary for the operation of these functions.

Assessment activities:

The following activities shall be performed:

- verify the correctness and completeness of the documentation by:
 - check for undocumented interfaces
- repeat the following steps for communication types public communication, adjacent communication and both at the same time:
 - disconnect or disable the corresponding communication type of the internet connected toys architectural component
 - wait at least 60 s
 - reconnect or enable the corresponding communication type
 - record the corresponding communication type
 - for each documented function:
 - monitor the operational status of the function
 - for each interface necessary for the operation of this function:
 - monitor the connection status;
 - record the time relative to the reconnection or enabling of the corresponding communication type, after which the internet connected toy indicates, that the interface is reconnected; or
 - record the time relative to the reconnection or enabling of the corresponding communication type, after which the interface was active at least once, and there is no indication that the internet connected toy has not resumed operation.

Assessment verdict:

The verdict PASS shall be assigned if:

- no indication, that the documentation is incorrect or incomplete, are found; and

- the internet connected toy signals resume of operations and establishment of all necessary communication channels within one hour; or
- all necessary communication channels of the architectural component were active at least once, and there is no indication that the internet connected toy has not resumed operation within one hour.
- The verdict FAIL shall be assigned otherwise.

Assessment evidence:

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

6.10.4 Assessment criteria for [AVAI-TIME-OUTA-NOT]

Assessment reference:

[\[AVAI-TIME-OUTA-NOT\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [AVAI-TIME-OUTA-NOT];
- a functional sufficiency assessment of the internet connected toys notification in case of non-availability induced by network resource restrictions, to fulfil [AVAI-TIME-OUTA-NOT];
- a functional sufficiency assessment of the internet connected toys notification in case of non-availability induced by DoS, to fulfil [AVAI-TIME-OUTA-NOT];

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- description how the status of the internet connected toys time sensitive functions can be read or deduced;
- a list of all time sensitive functions of the internet connected toy:
 - for each of these functions:
 - the time sensitive availability impact class;
 - whether the function needs network connectivity.
- CPU, memory, power and network resources available to the internet connected toy;
- demands on CPU, memory, power and network resources for workload consistent with the internet connected toys intended purpose and reasonably foreseeable use;
- a list of all notification mechanisms of the internet connected toy:
 - description how the notification mechanism can be configured.

The following test setups shall be prepared:

- the internet connected toy is set up in default configuration;
- configure at least one notification mechanism;
- a test setup to:
 - limit the network bandwidth between the internet connected toys architectural component and the internet connected toys RDPS to the internet;

- induce a denial-of-service status on the internet connected toy causing increasing demand on processing resources;
- receive notifications from the internet connected toy.

Assessment activities:

The following activities shall be performed:

- verify the correctness and completeness of the documentation;
- conceptually verify whether the documented notification mechanisms are suitable to send notifications in case of resource limitations;
- if at least on time sensitive function needs network connectivity:
 - progressively lower the network bandwidth available to the internet connected toys architectural component: and record any received notifications form the internet connected toy; and
 - progressively higher the intensity of requests to induce a denial-of-service status on the internet connected toy; and
 - record any received notifications form the internet connected toy.

Assessment verdict:

The verdict PASS shall be assigned if:

- no indication, that the documentation is incorrect or incomplete, are found;

and

- the internet connected toy sends notifications according to its configuration in case of non-availability of time sensitive function with IMP.AVAI.TIME.Medium or higher induced by DoS; or
- no time sensitive function with IMP.AVAI.TIME.Medium or higher was non-availability due to DoS;

and

- the internet connected toy sends notifications according to its configuration in case of non-availability of time sensitive function with IMP.AVAI.TIME.Medium or higher induced by network bandwidth limitation; or
- no time sensitive function with IMP.AVAI.TIME.Medium or higher was non-availability due to network bandwidth limitation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

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

6.10.5 Assessment criteria for [AVAI-TIME-PREV-NOT]

Assessment reference:

[\[AVAI-TIME-PREV-NOT\]](#)

Assessment objective:

The assessment covers:

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

- a functional sufficiency assessment of the internet connected toys notification in case of DoS, to fulfil [AVAI-TIME-PREV-NOT];

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of all time sensitive functions of the internet connected toy:
 - for each of these functions:
 - the time sensitive availability impact class;
 - whether the function needs network connectivity.
- CPU, memory, power and network resources available to the internet connected toy;
- demands on CPU, memory, power and network resources for workload consistent with the internet connected toys intended purpose and reasonably foreseeable use;
- a list of all notification mechanisms of the internet connected toy including a description on how the notification mechanism can be configured.

The following test setups shall be prepared:

- the internet connected toy is set up in default configuration;
- configure at least one notification mechanism;
- a test setup to:
 - read or deduced the status of the time sensitive functions from the internet connected toy;
 - limit the network bandwidth between the internet connected toys architectural component and the internet connected toys RDPS to the internet;
 - induce a DoS status on the internet connected toy causing increasing demand on processing resources;
 - receive notifications from the internet connected toy.

Assessment activities:

The following activities shall be performed:

- verify the correctness and completeness of the documentation;
- conceptually verify whether the documented notification mechanisms are suitable to send notifications in case of resource limitations;
- if at least on time sensitive function needs network connectivity:
 - progressively lower the network bandwidth available to the internet connected toys architectural component; and record any received notifications form the internet connected toy;
 - progressively higher the intensity of requests to induce a DoS status on the internet connected toy; and
 - record any received notifications form the internet connected toy.

Assessment verdict:

The verdict PASS shall be assigned if:

- no indication, that the documentation is incorrect or incomplete, are found; and

- the internet connected toy sends notifications according to its configuration in case of resource limitations induced by DoS; and
- the internet connected toy sends notifications according to its configuration in case of network bandwidth limitation; or
 - no time sensitive function with IMP.AVAI.TIME.High of the internet connected toy of the internet connected toy needs network connectivity.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

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

6.10.6 Assessment criteria for [AVAI-TIME-NET-PRIO]

Assessment reference:

[\[AVAI-TIME-NET-PRIO\]](#)

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- description how the status of the internet connected toys time sensitive functions can be read or deduced;
- a list of all time sensitive functions of the internet connected toy:
 - for each of these functions:
 - the time sensitive availability impact class;
 - whether the function needs network connectivity.
- prioritisation policy for the time sensitive functions of the internet connected toy in case of network resource conflict.

The following test setups shall be prepared:

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

Assessment activities:

The following activities shall be performed:

- verify the correctness and completeness of the documentation;

- conceptually verify the prioritisation policy;
- progressively lower the network bandwidth available to the internet connected toy's architectural component:
 - record the status of every time sensitive function.

Assessment verdict:

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

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

6.10.7 Assessment criteria for [AVAI-TIME-RES-PRIO]

Assessment reference:

[\[AVAI-TIME-RES-PRIO\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [AVAI-TIME-RES-PRIO];
- a functional sufficiency assessment of the internet connected toys resource prioritisation in case of non-availability induced by DoS, to fulfil [AVAI-TIME-RES-PRIO]

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- description how the status of the internet connected toys time sensitive functions can be read or deduced;
- a list of all time sensitive functions of the internet connected toy:
 - for each of these functions:
 - the time sensitive availability impact class;
 - whether the function needs network connectivity.
- prioritisation policy for the time sensitive functions of the internet connected toy in case of CPU, memory or power resource conflict.

The following test setups shall be prepared:

- the internet connected toy is set up in default configuration;
- a test setup to:
 - read or deduced the status of the time sensitive functions from the internet connected toy;
 - induce a DoS status on the internet connected toy causing increasing demand on processing resources.

Assessment activities:

The following activities shall be performed:

- verify the correctness and completeness of the documentation;
- conceptually verify the prioritisation policy;
- progressively higher the intensity of requests to induce a DoS status on the internet connected toy:
 - record the status of every time sensitive function.

Assessment verdict:

The verdict PASS shall be assigned if:

- no indication, that the documentation is incorrect or incomplete, are found; and
- the prioritisation policy is conceptually valid; and
- every time sensitive function:
 - the status of the function is in accordance with the prioritisation policy during DoS.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

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

6.10.8 Assessment criteria for [AVAI-TIME-DOS-RATE]

Assessment reference:

[\[AVAI-TIME-DOS-RATE\]](#)

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of all time sensitive function of the internet connected toy:
 - for each of these functions:
 - the time sensitive availability impact class;
 - a list of all used interfaces.
- a list of all machine interface provided by the internet connected toy;
- rate limiting policy for the internet connected toy.

The following test setups shall be prepared:

- the internet connected toy is set up in default configuration;

- a test setup to:
 - induce a DoS status on the internet connected toy causing increasing demand on processing resources;
 - check the status of all time sensitive function with IMP.AVAI.TIME.High.

Assessment activities:

The following activities shall be performed:

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

Assessment verdict:

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

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

6.10.9 Assessment criteria for [AVAI-SUM-SCHEDULE]

Assessment reference:

[\[AVAI-SUM-SCHEDULE\]](#)

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of all time sensitive functions of the internet connected toy:
 - for each of these functions:
 - the time sensitive availability impact class.
- a list of all software update mechanisms of the internet connected toy:
 - for each of these mechanisms:
 - whether this mechanism can effect at least one time sensitive function with IMP.AVAI.TIME.Medium or higher;

- description how the software update mechanism can be configured.

The following test setups shall be prepared:

- the internet connected toy is set up in default configuration.

Assessment activities:

The following activities shall be performed:

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

Assessment verdict:

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

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

6.11 Non-interference

6.11.1 Assessment criteria for [NOINF-AMP]

Assessment reference:

[\[AVAI-TIME-NET-PRIO\]](#)

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of all function, whose use can impact the availability of other devices, services or networks of the internet connected toy:
 - for each of these functions:
 - the function, whose use can impact the availability of other devices, services or networks impact class;
 - a list of all used interfaces.

The following test setups shall be prepared:

- the internet connected toy is set up in default configuration;
- a test setup to:
 - execute amplification attacks against the internet connected toy;
 - measure the affective amplification of network traffic caused by the internet connected toy.

Assessment activities:

The following activities shall be performed:

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

Assessment verdict:

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

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

6.12 Attack surface minimisation

6.12.1 Assessment criteria for [LAS-INVAL]

Assessment reference:

[\[LAS-INVAL\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [LAS-INVAL];
- a functional sufficiency assessment of the input validation mechanisms used by the internet connected toy to fulfil [LAS-INVAL];

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for each internet connected toy's function that uses external data input:
 - a list of all interfaces over which these functions can receive external data input, including their communication type;
 - a description of the internet connected toy's input validation mechanisms.

The following test setups shall be prepared:

- For each internet connected toy's functions that use external data input:
 - For each interfaces over which these functions can receive external data input:
 - a test setup to send external data input that does not meet a input validation mechanism's acceptance pattern based on a sample internet connected toy in default configuration.

Assessment activities:

- For each internet connected toy's function that uses external data input, the internet connected toy's conformity to [LAS-INVAL] shall be validated based on the documentation by:
 - For each interface over which these functions can receive external data input:
 - Verify whether the interface has COM.StrictLocal:
 - For each interface that does not have COM.StrictLocal:
 - verify the existence of input validation mechanisms
- For each input validation mechanism, its correct implementation shall be verified by:
 - sending data input that does not meet a input validation mechanism's acceptance pattern and assessing the internet connected toy's behaviour.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [LAS-INVAL]; and
- the verification of the correct implementation of each input validation mechanism was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each input validation mechanism.

6.12.2 Assessment criteria for [LAS-INSAN]

Assessment reference:

[\[LAS-INSAN\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [LAS-INSAN];
- a functional sufficiency assessment of the input sanitisation mechanisms used by the internet connected toy to fulfil [LAS-INSAN];

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for each internet connected toy's function that uses external data input:
 - a description of the internet connected toy's input sanitisation mechanisms, or
 - an explanation of the input validation mechanisms capability to prevent potential incidents triggered by external data input.

The following test setups shall be prepared:

- For each internet connected toy's functions that use external data input:
 - For each interfaces over which these functions can receive external data input:
 - a test setup to send external data input that includes common code injection patterns based on a sample internet connected toy in default configuration.

Assessment activities:

- For each internet connected toy's function that uses external data input, the internet connected toy's conformity to [LAS-INSAN] shall be validated based on the documentation by:
 - For each interface over which these functions can receive external data input:
 - verify the existence of input sanitisation mechanisms; or
 - verify that the explanation of the input validation mechanisms capability to prevent potential incidents triggered by external data input.
- For each input sanitisation mechanism, its correct implementation shall be verified by:
 - sending data input that include common code injection patterns and assessing the internet connected toy's behaviour.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [LAS-INSAN]; and
- the verification of the correct implementation of each input sanitisation mechanism was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;

- descriptions of the performed tests and records of performed tests to verify the correct implementation of each input sanitisation mechanism.

6.12.3 Assessment criteria for [LAS-PHY-INF]

Assessment reference:

[\[LAS-PHY-INF\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [LAS-PHY-INF] and,
- a functional completeness assessment on the internet connected toy's capabilities that are addressed by [LAS-PHY-INF].

Assessment preparation:

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

- a list of all physical interfaces that are provided by hardware architectural components; and
- for each physical interface:
 - a justification for its necessity for the internet connected toy's intended purpose.

The following test setup shall be prepared:

- hardware architectural components; and
- appropriate inspection equipment and tools to identify physical interfaces, including those potentially concealed behind covers, seals, etc.

Assessment activities:

- The internet connected toy's conformity to [LAS-PHY-INF] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by inspecting the hardware architectural components.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [LAS-PHY-INF]; and
- the verification of the correctness and completeness of the documentation was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- photographs/annotated drawings of all discovered physical interfaces;
- records of the validation of the documentation;
- descriptions of the performed inspection.

6.12.4 Assessment criteria for [LAS-LOGIC-INF]

Assessment reference:

[\[LAS-LOGIC-INF\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [LAS-LOGIC-INF]; and
- a functional completeness assessment on the internet connected toy's capabilities that are addressed by [LAS-LOGIC-INF].

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of all logical interfaces that are provided by default; and
- for each logical interface provided by default:
 - a justification for its necessity for the internet connected toy's intended purpose.

The following test setup shall be prepared:

- a test setup for identifying logical interfaces based on a sample internet connected toy in default configuration.

NOTE: Such a test setup can amongst others include network scanning tools, protocol-specific discovery tools (e.g. for UPnP discovery) and API probing tools.

Assessment activities:

- The internet connected toy's conformity to [LAS-LOGIC-INF] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by inspecting the internet connected toy.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [LAS-LOGIC-INF]; and
- the verification of the correctness and completeness of the documentation was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- raw & annotated scan results;
- screenshots/logs of discovery attempts for logical interfaces.

6.12.5 Assessment criteria for [LAS-APP]

Assessment reference:

[\[LAS-APP\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [LAS-APP]; and
- a functional completeness assessment on the internet connected toy's capabilities that are addressed by [LAS-APP];

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a list of all application software that are installed by default; and

NOTE 1: This information might be extractable from a internet connected toy's SBOM.

- for each application software installed by default:
 - a justification for its necessity for the the internet connected toy intended purpose.

The following test setup shall be prepared:

- a test setup for identifying application software installed at the internet connected toy based on a sample internet connected toy in default configuration.

NOTE 2: Such a test setup can amongst others include means to identify installed application software based on inspecting the internet connected toy's interfaces and application software discovery tool results such as software binary analysis tools or source code analysis tools.

Assessment activities:

- The internet connected toy's conformity to [LAS-APP] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by inspecting the internet connected toy.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [LAS-APP]; and
- the verification of the correctness and completeness of the documentation was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- raw & annotated application software discovery tool results;
- screenshots/logs of discovery attempts for installed application software via the internet connected toy's interfaces.

6.12.6 Assessment criteria for [LAS-SBOOT]

Assessment reference:

[\[LAS-SBOOT\]](#)

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- 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;
- documentation on how the bootloader function verifies the integrity and authenticity of the hardware architectural component's software.

The following test setup shall be prepared:

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

Assessment activities:

- The internet connected toy's conformity to [LAS-SBOOT] shall be validated based on the documentation.
- The correct implementation of the bootloader function's integrity and authenticity verification of core software shall be verified based on:
 - tampering the integrity and authenticity of installed core software or installing integrity and authenticity tampered core software; and
 - restarting the internet connected toy's hardware architectural component.

NOTE: Typical results are:

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

either halts, resets, or boots into a secure fallback; and

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

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [LAS-SBOOT]; and
- the internet connected toy's hardware architectural component does not execute the modified core software.

Otherwise, the verdict FAIL shall be assigned.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and documentation of associated test records that verify the correct implementation of the bootloader function's integrity and authenticity verification.

6.13 Exploit mitigation

6.13.1 Assessment criteria for [PRIV-DATA-HIGH]

Assessment reference:

[\[PRIV-DATA-HIGH\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [PRIV-DATA-HIGH];
- a functional sufficiency assessment of the internet connected toy's mechanisms that ensure conformity with [PRIV-DATA-HIGH].

Assessment preparation:

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

- a list of the internet connected toy's architectural components;
- for each internet connected toy's architectural component:
 - a list of processed data assets that are:
 - confidential data with [IMP.CONF.High]; or
 - integrity relevant data with [IMP.INT.High]; and
 - a description of the processes running on the same hardware as the architectural component that have privileges to access the listed data assets, including a justification for the necessity for the internet connected toy's intended purpose;
 - a description of the mechanisms that ensure conformity with [PRIV-DATA-HIGH].

The following test setups shall be prepared:

- for each architectural component, a test setup for accessing confidential data with [IMP.CONF.High] and integrity relevant data with [IMP.INT.High] via unauthorised processes running on the same hardware.

Assessment activities:

- The internet connected toy's conformity to [PRIV-DATA-HIGH] shall be validated based on the documentation.
- For each architectural component, the correct implementation the mechanisms that ensure conformity with [PRIV-DATA-HIGH] shall be verified by:
 - trying to access confidential data with [IMP.CONF.High] or integrity relevant data with [IMP.INT.High] via unauthorised processes.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [PRIV-DATA-HIGH]; and
- the verification of the correct implementation of the mechanisms that ensure conformity with [PRIV-DATA-HIGH] was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation the mechanisms that ensure conformity with [PRIV-DATA-HIGH].

6.13.2 Assessment criteria for [PRIV-FUNC-HIGH]

Assessment reference:

[\[PRIV-FUNC-HIGH\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [PRIV-FUNC-HIGH];
- a functional sufficiency assessment of the internet connected toy's mechanisms that ensure conformity with [PRIV-FUNC-HIGH].

Assessment preparation:

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

- a list of the internet connected toy's architectural components;
- for each internet connected toy's architectural component:
 - a list of provided function assets that are:
 - time sensitive function of [IMP.AVAI.TIME.High];
 - integrity relevant function of [IMP.INT.High]; or
 - function, whose use can cause harm of [IMP.FH.High]; and
 - a description of the processes running on the same hardware as the architectural component that have privileges to access the listed function assets, including a justification for the necessity for the internet connected toy's intended purpose;
 - a description of the mechanisms that ensure conformity with [PRIV-FUNC-HIGH].

The following test setups shall be prepared:

- for each architectural component, a test setup for accessing time sensitive function with [IMP.AVAI.TIME.High], integrity relevant function with [IMP.INT.High] function, whose use can cause harm and [IMP.FH.High] via unauthorised processes running on the same hardware.

Assessment activities:

- The internet connected toy's conformity to [PRIV-FUNC-HIGH] shall be validated based on the documentation.
- For each architectural component, the correct implementation the mechanisms that ensure conformity with [PRIV-FUNC-HIGH] shall be verified by:
 - trying to access time sensitive function with [IMP.AVAI.TIME.High], integrity relevant function with [IMP.INT.High] function, whose use can cause harm or [IMP.FH.High] via unauthorised processes.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity to [PRIV-FUNC-HIGH]; and
- the verification of the correct implementation of the mechanisms that ensure conformity with [PRIV-FUNC-HIGH] was successful.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation the mechanisms that ensure conformity with [PRIV-FUNC-HIGH].

6.14 Monitoring

6.14.1 Assessment criteria for [MON-LOW]

Assessment reference:

[\[MON-LOW\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [MON-LOW];
- a functional sufficiency assessment of monitoring mechanisms used by the internet connected toy to fulfil [MON-LOW];

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- list of all monitoring mechanisms;
- documentation on how the monitoring mechanisms creates audit event data;
- documentation which audit event data are created by which monitoring mechanism.

The following test setups shall be prepared:

- a test user with the necessary permissions has been set up to trigger the events listed in [MON-LOW];
- monitoring mechanism are enabled on the internet connected toy such that at least all the events in [MON-LOW] are covered;
- a test setup for triggering the events listed in [MON-LOW].

Assessment activities:

The following activities shall be performed:

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

Assessment verdict:

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

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

6.14.2 Assessment criteria for [MON-MEDIUM]

Assessment reference:

[\[MON-MEDIUM\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [MON-MEDIUM];
- a functional sufficiency assessment of monitoring mechanisms used by the internet connected toy to fulfil [MON-MEDIUM];

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- list of all monitoring mechanisms;
- documentation on how the monitoring mechanisms creates audit event data;
- documentation which audit event data are created by which monitoring mechanism.

The following test setups shall be prepared:

- a test user with the necessary permissions has been set up to trigger the events listed in [MON-MEDIUM];
- a test setup for triggering the events listed in [MON-MEDIUM].

Assessment activities:

The following activities shall be performed:

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

Assessment verdict:

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- descriptions of the performed tests and records of performed tests

6.14.3 Assessment criteria for [MON-HIGH]

Assessment reference:

[\[MON-HIGH\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [MON-HIGH];
- a functional sufficiency assessment of monitoring mechanisms used by the internet connected toy to fulfil [MON-HIGH];

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- list of all monitoring mechanisms;
- documentation on how the monitoring mechanisms creates audit event data;
- documentation which audit event data are created by which monitoring mechanism.

The following test setups shall be prepared:

- a test user with the necessary permissions has been set up to trigger the events listed in [MON-HIGH];
- a test setup for triggering the events listed in [MON-HIGH].

Assessment activities:

The following activities shall be performed:

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

Assessment verdict:

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

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

6.14.4 Assessment criteria for [MON-HANDLE]

Assessment reference:

[\[MON-HANDLE\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of each audit event data generated by a monitoring mechanism of the internet connected toy to fulfil [MON-HANDLE],

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for each architectural component:
 - documentation on support of public communication;
 - list of all audit event data generated by a monitoring mechanism and for each entry:
 - corresponding logging mechanism or data transfer mechanism.

The following test setups shall be prepared:

- for each logging mechanism in *assessment preparation*, a test setup that allows to:
 - generate audit event data;
 - access the storage location where logging data is stored.
- for each data transfer mechanism in *assessment preparation*, a test setup that allows to:
 - generate audit event data;
 - access the architectural component or other device where the data is transferred to.

Assessment activities:

The following activities shall be performed:

- For each audit event data listed in *assessment preparation* with assigned logging mechanism:
 - verify that the assigned logging mechanism is enabled;
 - generate audit event data; and
 - check that the logging data produced by the logging mechanism from the audit event data is generated and stored.
- For each audit event data listed in *assessment preparation* with assigned data transfer mechanism:
 - check that the corresponding architectural component does not support public communication;
 - verify that the assigned data transfer mechanism is enabled;
 - generate audit event data; and
 - check that the audit event data is transferred to the destination (architectural component or other device).

Assessment verdict:

The verdict PASS shall be assigned if:

- The documentation indicates the internet connected toy's conformity with [MON-HANDLE];
- for every audit event data assigned to a logging mechanism corresponding logging data is generated and stored; and
- for every audit event data assigned to a data transfer mechanism:
 - the corresponding architectural component does not support public communication; and
 - audit event data is transferred to the destination.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

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

6.14.5 Assessment criteria for [LOG-TIME]**Assessment reference:**

[\[LOG-TIME\]](#)

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- documentation on how the logging mechanisms creates logging data;
- documentation for which events logging data are created by which logging mechanism;
- documentation on where logging data are stored;
- documentation on the time sources and formats used by logging mechanism.

The following test setups shall be prepared:

- a test user with the necessary permissions has been set up to trigger the events;
- logging mechanism are enabled on the internet connected toy such that at least all the events in the following point are covered;
- a test setup for triggering events as described in *Assessment preparation* in clause [6.14.1](#) or clause [6.14.2](#).

Assessment activities:

The following activities shall be performed:

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

Assessment verdict:

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

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

6.14.6 Assessment criteria for [LOG-TIME-HIGH]

Assessment reference:

[\[LOG-TIME-HIGH\]](#)

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- documentation on how the logging mechanisms creates logging data;
- documentation for which events logging data are created by which logging mechanism;
- documentation on where logging data are stored;
- documentation on the time sources and formats used by logging mechanism.

The following test setups shall be prepared:

- a test user with the necessary permissions has been set up to trigger the events;
- logging mechanism are enabled on the internet connected toy such that at least all the events in the following point are covered;
- a test setup for triggering events as described in *Assessment preparation* in clause [6.14.3](#).

Assessment activities:

The following activities shall be performed:

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

Assessment verdict:

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- descriptions of the performed tests and records of performed tests

6.14.7 Assessment criteria for [LOG-STORE-MEDIUM]

Assessment reference:

[\[LOG-STORE-MEDIUM\]](#)

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- list of all audit event data and for each entry:
 - documentation on which logging mechanism is used to generate and store corresponding logging data;
 - documentation on how the corresponding logging mechanism generates logging data; and
 - documentation on where logging data are stored;
 - documentation and reasoning on how many entries of this architectural component can be stored.

The following test setups shall be prepared:

- a test user with the necessary permissions has been set up to trigger the generation of audit event data;
- logging mechanisms are enabled on the internet connected toy such that at least all the events listed in [LOG-STORE-MEDIUM] (clause [5.14.2](#)) are covered;
- a test setup for triggering the generation of audit event data as described in *Assessment preparation* in [LOG-STORE-MEDIUM] (clause [6.14.2](#)).

Assessment activities:

The following activities shall be performed:

- For each audit event data listed in *Assessment preparation*:
 - verify the reasoning for the number of stored entries of this architectural component;
 - trigger the generation of the audit event data;
 - trigger the generation of further audit event data for the same architectural component to reach the value before deletion or rotation as documented in *assessment preparation*; and
 - verify whether the logging data associated with the first audit event data is still present or a user notification informed about deletion or rotation.

Assessment verdict:

The verdict PASS shall be assigned if:

- for each audit event data listed in *Assessment preparation* that could be used by logging mechanisms:
 - the reasoning for the number of stored entries of this architectural component is verified; and
 - the logging data is still present after generation of further audit event data; or
 - user notification informed about deletion or rotation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

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

6.14.8 Assessment criteria for [LOG-STORE-HIGH]

Assessment reference:

[\[LOG-STORE-HIGH\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of logging mechanisms used by the internet connected toy to fulfil [LOG-STORE-HIGH],

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- list of all audit event data and for each entry:
 - documentation on which logging mechanism is used to generate and store corresponding logging data;
 - documentation on how the corresponding logging mechanism generates logging data; and
 - documentation on where logging data are stored;
 - documentation and reasoning on how many entries of this architectural component can be stored.

The following test setups shall be prepared:

- a test user with the necessary permissions has been set up to trigger the generation of audit event data;
- logging mechanisms are enabled on the internet connected toy such that at least all the events listed in [LOG-STORE-HIGH] (clause [5.14.3](#)) are covered;
- a test setup for triggering the generation of audit event data as described in *Assessment preparation* in [LOG-STORE-HIGH] (clause [6.14.3](#)).

Assessment activities:

The following activities shall be performed:

- For each audit event data listed in *Assessment preparation*:
 - verify the reasoning for the number of stored entries of this architectural component;
 - trigger the generation of the audit event data;
 - trigger the generation of further audit event data for the same architectural component to reach the value before deletion or rotation as documented in *assessment preparation*; and
 - verify whether the logging data associated with the first audit event data is still present or a user notification informed about deletion or rotation.

Assessment verdict:

The verdict PASS shall be assigned if:

- for each audit event data listed in *Assessment preparation* that could be used by logging mechanisms:
 - the reasoning for the number of stored entries of this architectural component is verified; and

- the logging data is still present after generation of further audit event data; or
- user notification informed about deletion or rotation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

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

6.14.9 Assessment criteria for [LOG-CONFIG]

Assessment reference:

[\[LOG-CONFIG\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [LOG-CONFIG];
- a functional sufficiency assessment of each logging mechanism used by the internet connected toy to fulfil [LOG-CONFIG],

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- a description of each logging mechanism, including:
 - which audit event data can be processed;
 - which logging data are generated;
 - where the generated logging data is stored;
 - where and how to disable the {SupportingFunctionality:LoggingMechanism}.

The following test setups shall be prepared:

- a test setup that allows to identify logging mechanisms on a sample internet connected toy in default configuration;
- for each logging mechanism, a test setup that allows to:
 - generate audit event data;
 - access the storage location where logging data is stored;
 - see the user interaction steps (e.g. menu, dialog, confirmation after deletion).

Assessment activities:

The following activities shall be performed:

- The internet connected toy's conformity to [LOG-CONFIG] shall be validated based on the documentation.
- The correctness of the documentation shall be verified by checking that all documented logging mechanisms have an option to be disabled:
 - For each logging mechanism, its possibility to be disabled shall be verified by:
 - generating audit event data;

- check that corresponding logging data is generated (and stored) by the logging mechanism;
- disable the logging mechanism as documented; and
- check that generating audit event data no longer leads to logging data generated (and stored) by the logging mechanism.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity with [LOG-CONFIG]; and
- the verification of the correctness of the documentation was successful; and
- all logging mechanisms have a possibility to be disabled.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correctness of the documentation.

6.15 Factory reset and data portability

6.15.1 Assessment criteria for [DLM-PERM]

Assessment reference:

[\[DLM-PERM\]](#)

Assessment objective:

The assessment covers:

- a conceptual assessment of [DLM-PERM];
- a functional completeness assessment on the internet connected toy's capabilities that are addressed by [DLM-PERM]; and
- a functional sufficiency assessment of each deletion mechanism used by the internet connected toy to fulfil [DLM-PERM].

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

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

The following test setups shall be prepared:

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

Assessment activities:

The following activities shall be performed:

- The internet connected toy's conformity to [DLM-PERM] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by checking that all documented deletion mechanisms are implemented:
 - for each deletion mechanism, its correct implementation shall be verified by:
 - generating user-related data and installing an application as a user;
 - deleting the generated user-related data and the application; and
 - checking whether the:
 - user-related data and the application are permanently removed, e.g. by at least checking the storage location of the user-related data and application before and after deletion;
 - deletion mechanism is easy to use with limited technical knowledge;
 - user can only delete its own data in multi-user systems; and
 - user is provided with clear confirmation of deletion after user-related data or a user-installed application have been deleted.
- Over all deletion mechanisms, it is to be checked whether all generated sample user-related data and installed applications can be permanently removed.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the internet connected toy's conformity with [DLM-PERM]; and
- the verification of the correctness and completeness of the documentation was successful; and
- the verification of the correct implementation of each deletion mechanism was successful; and
- all deletion mechanisms are able to permanently remove all generated user-related data and user-installed applications.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correctness and completeness of the documentation;

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

Annex A (informative): Relationship between the present document and the essential cybersecurity requirements of EU Regulation (EU) 2024/2847

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

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

**Table A.1: Relationship between the present document and
the requirements of Regulation (EU) 2024/2847 - the Cyber Resilience Act**

Description	Essential Requirements of Regulation (EU) 2024/2847	Clause(s) of the present document	Remarks / Notes
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)	[ACM-FH] 5.6.1, 6.6.1 [AUM-FH] 5.6.3, 6.6.3 [AUTHZ-LP] 5.6.4, 6.6.4 [AUTHZ-R] 5.6.5, 6.6.5 [AUTHZ-PC] 5.6.6, 6.6.6 [AVAI-TIME-RECO-POW] 5.10.1, 6.10.1 [AVAI-TIME-NETW] 5.10.2, 6.10.2 [AVAI-TIME-RECO-NETW] 5.10.3, 6.10.3 [AVAI-TIME-OUTA-NOT] 5.10.4, 6.10.4 [AVAI-TIME-PREV-NOT] 5.10.5, 6.10.5 [AVAI-TIME-NET-PRIO] 5.10.6, 6.10.6 [AVAI-TIME-RES-PRIO] 5.10.7, 6.10.7 [AVAI-TIME-DOS-RATE] 5.10.8, 6.10.8 [AVAI-SUM-SCHEDULE] 5.10.9, 6.10.9 [BACKUP-TRANS] 5.2.4, 6.2.4 [BACKUP-AUTOTRANS] 5.2.5, 6.2.5 [BACKUP-EXPORT] 5.2.6, 6.2.6 [CONF-SSM] 5.7.1, 6.7.1 [CONF-COM] 5.7.2, 6.7.2 [CRY-GENERAL] 5.4.7, 6.4.7 [CRY-CCK-PRE-LEN] 5.4.8, 6.4.8 [CRY-CCK-GEN] 5.4.9, 6.4.9 [CRY-PW-PRE-COM] 5.4.10, 6.4.10 [CRY-PW-GEN-COM] 5.4.11, 6.4.11 [CRY-PW-USR-COM] 5.4.12, 6.4.12 [DLM-PERM] 5.15.1, 6.15.1 [DMIN-DJST] 5.9.1, 6.9.1 [PRIV-DATA-HIGH] 5.13.1, 6.13.1 [PRIV-FUNC-HIGH] 5.13.2, 6.13.2 [GUI-SECCONF] 5.2.3, 6.2.3 [INT-SSM] 5.8.1, 6.8.1 [INT-COM] 5.8.2, 6.8.2 [INT-SWPCK] 5.8.3, 6.8.3 [LAS-INVAL] 5.12.1, 6.12.1 [LAS-INSAN] 5.12.2, 6.12.2 [LAS-PHY-INF] 5.12.3, 6.12.3 [LAS-LOGIC-INF] 5.12.4, 6.12.4 [LAS-APP] 5.12.5, 6.12.5 [LAS-SBOOT] 5.12.6, 6.12.6 [MON-LOW] 5.14.1, 6.14.1	

Description	Essential Requirements of Regulation (EU) 2024/2847	Clause(s) of the present document	Remarks / Notes
		[MON-MEDIUM] 5.14.2, 6.14.2 [MON-HIGH] 5.14.3, 6.14.3 [MON-HANDLE] 5.14.4, 6.14.4 [LOG-TIME] 5.14.5, 6.14.5 [LOG-TIME-HIGH] 5.14.6, 6.14.6 [LOG-STORE-MEDIUM] 5.14.7, 6.14.7 [LOG-STORE-HIGH] 5.14.8, 6.14.8 [LOG-CONFIG] 5.14.9, 6.14.9 [NKEV-MKAV] 5.3.1, 6.3.1 [NKEV-INIT-UDP] 5.3.2, 6.3.2 [NOINF-AMP] 5.11.1, 6.11.1 [PARCONT] 5.6.2, 6.6.2 [SDC-AUM-FH] 5.4.1, 6.4.1 [SDC-SUM-AUTO] 5.4.2, 6.4.2 [SDC-SUM-NOTIF] 5.4.3, 6.4.3 [SDC-FRM] 5.4.4, 6.4.4 [SDC-PARCONT] 5.4.5, 6.4.5 [SDC-MON-HANDLE] 5.4.6, 6.4.6 [SU-SUPPORT] 5.5.1, 6.5.1 [SU-PROVIDE] 5.5.2, 6.5.2 [SU-AUTO] 5.5.3, 6.5.3 [SU-DISABLE-AUTO] 5.5.4, 6.5.4 [SU-POSTPONE-AUTO] 5.5.5, 6.5.5 [SU-NOTIF] 5.5.6, 6.5.6 [USERNOT-NOSECFUC] 5.2.1, 6.2.1 [USERNOT-SECREL] 5.2.2, 6.2.2	
Products with digital elements are made available on the market without known exploitable vulnerabilities.	Annex I, Part I, (2)(a)	[NKEV-MKAV] 5.3.1, 6.3.1 [NKEV-INIT-UDP] 5.3.2, 6.3.2	
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)	[CRY-GENERAL] 5.4.7, 6.4.7 [CRY-CCK-PRE-LEN] 5.4.8, 6.4.8 [CRY-CCK-GEN] 5.4.9, 6.4.9 [CRY-PW-PRE-COM] 5.4.0, 6.4.10 [CRY-PW-GEN-COM] 5.4.1, 6.4.11 [CRY-PW-USR-COM] 5.4.2, 6.4.12 [LAS-LOGIC-INF] 5.12.4, 6.12.4 [LAS-APP] 5.12.5, 6.12.5 [SDC-AUM-FH] 5.4.1, 6.4.1 [SDC-SUM-AUTO] 5.4.2, 6.4.2 [SDC-SUM-NOTIF] 5.4.3, 6.4.3 [SDC-FRM] 5.4.4, 6.4.4 [SDC-PARCONT] 5.4.5, 6.4.5 [SDC-MON-HANDLE] 5.4.6, 6.4.6	
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)	[SDC-SUM-AUTO] 5.4.2, 6.4.2 SDC-SUM-NOTIF] 5.4.3, 6.4.3 [SU-SUPPORT] 5.5.1, 6.5.1 [SU-PROVIDE] 5.5.2, 6.5.2 [SU-AUTO] 5.5.3, 6.5.3 [SU-DISABLE-AUTO] 5.5.4, 6.5.4 [SU-POSTPONE-AUTO] 5.5.5, 6.5.5 [SU-NOTIF] 5.5.6, 6.5.6	

Description	Essential Requirements of Regulation (EU) 2024/2847	Clause(s) of the present document	Remarks / Notes
Products with digital elements ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access.	Annex I, Part I, (2)(e)	[ACM-FH] 5.6.1 , 6.6.1 [AUM-FH] 5.6.3 , 6.6.3 [AUTHZ-LP] 5.6.4 , 6.6.4 [AUTHZ-R] 5.6.5 , 6.6.5 [AUTHZ-PC] 5.6.6 , 6.6.6 [MON-MEDIUM] 5.14.2 , 6.14.2 [MON-HIGH] 5.14.3 , 6.14.3 [LOG-TIME] 5.14.5 , 6.14.5 [LOG-TIME-HIGH] 5.14.6 , 6.14.6 [PARCONT] 5.6.2 , 6.6.2 [SDC-AUM-FH] 5.4.1 , 6.4.1	
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)	[ACM-FH] 5.6.1 , 6.6.1 [AUM-FH] 5.6.3 , 6.6.3 [AUTHZ-LP] 5.6.4 , 6.6.4 [AUTHZ-R] 5.6.5 , 6.6.5 [AUTHZ-PC] 5.6.6 , 6.6.6 [CONF-SSM] 5.7.1 , 6.7.1 [CONF-COM] 5.7.2 , 6.7.2	
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 authorised by the user, and report on corruptions.	Annex I, Part I, (2)(f)	[ACM-FH] 5.6.1 , 6.6.1 [AUM-FH] 5.6.3 , 6.6.3 [AUTHZ-LP] 5.6.4 , 6.6.4 [AUTHZ-R] 5.6.5 , 6.6.5 [AUTHZ-PC] 5.6.6 , 6.6.6 [INT-SSM] 5.8.1 , 6.8.1 [INT-COM] 5.8.2 , 6.8.2 [INT-SWPCK] 5.8.3 , 6.8.3 [MON-LOW] 5.14.1 , 6.14.1 [MON-MEDIUM] 5.14.2 , 6.14.2 [MON-HIGH] 5.14.3 , 6.14.3	
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 minimisation).	Annex I, Part I, (2)(g)	[DMIN-DJST] 5.9.1 , 6.9.1	
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] 5.10.1 , 6.10.1 [AVAI-TIME-NETW] 5.10.2 , 6.10.2 [AVAI-TIME-RECO-NETW] 5.10.3 , 6.10.3 [AVAI-TIME-OUTA-NOT] 5.10.4 , 6.10.4 [AVAI-TIME-PREV-NOT] 5.10.5 , 6.10.5 [AVAI-TIME-NET-PRIO] 5.10.6 , 6.10.6 [AVAI-TIME-RES-PRIO] 5.10.7 , 6.10.7 [AVAI-TIME-DOS-RATE] 5.10.8 , 6.10.8 [AVAI-SUM-SCHEDULE] 5.10.9 , 6.10.9	
Products with digital elements minimise 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)	[NOINF-AMP] 5.11.1 , 6.11.1	
Products with digital elements are designed, developed and produced to limit attack surfaces, including external interfaces.	Annex I, Part I, (2)(j)	[LAS-INVAL] 5.12.1 , 6.12.1 [LAS-INSAN] 5.12.2 , 6.12.2 [LAS-PHY-INF] 5.12.3 , 6.12.3 [LAS-LOGIC-INF] 5.12.4 , 6.12.4 [LAS-APP] 5.12.5 , 6.12.5 [LAS-SBOOT] 5.12.6 , 6.12.6	

Description	Essential Requirements of Regulation (EU) 2024/2847	Clause(s) of the present document	Remarks / Notes
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] 5.10.1 , 6.10.1 [AVAI-TIME-NET-PRIO] 5.10.6 , 6.10.6 [AVAI-TIME-RES-PRIO] 5.10.7 , 6.10.7 [PRIV-DATA-HIGH] 5.13.1 , 6.13.1 [PRIV-FUNC-HIGH] 5.13.2 , 6.13.2	
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)	[MON-LOW] 5.14.1 , 6.14.1 [MON-MEDIUM] 5.14.2 , 6.14.2 [MON-HIGH] 5.14.3 , 6.14.3 [MON-HANDLE] 5.14.4 , 6.14.4 [LOG-TIME] 5.14.5 , 6.14.5 [LOG-TIME-HIGH] 5.14.6 , 6.14.6 [LOG-STORE-MEDIUM] 5.14.7 , 6.14.7 [LOG-STORE-HIGH] 5.14.8 , 6.14.8 [LOG-CONFIG] 5.14.9 , 6.14.9 [SDC-MON-HANDLE] 5.4.6 , 6.4.6 [SU-DISABLE-AUTO] 5.5.4 , 6.5.4 [SU-POSTPONE-AUTO] 5.5.5 , 6.5.5 [SU-NOTIF] 5.5.6 , 6.5.6 [USERNOT-NOSECFUC] 5.2.1 , 6.2.1	
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] 5.15.1 , 6.15.1 [SDC-FRM] 5.4.4 , 6.4.4	

Key to columns:

Description A textual reference to the requirement.

Requirements of Regulation

Identification of point(s) defining the requirement in Regulation (EU) 2024/2847 - the Cyber Resilience Act.

Clause(s) of the present document

Identification of clause(s) addressing the requirement in the present document

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

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

Annex B (informative): Security analysis

B.1 General

This Annex documents the security analysis on which the present document is based on.

B.2 Assets

The present document uses the categories data assets and function assets to classify the different assets. Different items of those asset categories are typically interlinked, e.g. in general:

- function assets can create, modify, use, delete, communicate or otherwise process data assets,
- function assets can trigger other function assets,
- data assets can control function assets and
- executable code that implements function assets is a data asset (here function binary data).

The function assets addressed by the present document are listed in clause [4.1.1](#).

The data assets addressed by the present document are listed in clause [4.1.2](#).

B.3 Risk factors

The present document uses the categories impact and attack surface to classify the risk factors.

The attack surface parameter used by the present document are:

- physical operational environment - [POE], where details are described in clause [4.3.2](#).
- logical operational environment - [LOE] expressed in terms of possible communication types - [COM], where details are described in clause [4.3.3](#).
- interface - [IF], where details are described in clause [4.3.4](#).
- users, where details are described in clause [4.5](#).

The impact parameter used by the present document are:

- impact classes - [IMP] assigned to the data assets and function asset provided in clause [4.1](#). The impact class assignment is provided in annex [D](#).

Those risk factors are used to determine the applicability of the technical requirements and their corresponding details.

B.4 Assumptions

The present document assumes that internet connected toys are used according to their intended purpose and reasonably foreseeable use.

B.5 Threats

The present document addresses the threats scenarios described by the columns *Threat Actor*, *Threat Action*, *Asset*, and *Threat Details* of table [B.1](#).

B.6 Relationship between the present document and the covered/not covered cybersecurity risks

The table [B.1](#) amends the threat scenarios considered by the related risk factors, corresponding mitigation measures and a statement on the acceptability of residual risk.

Table B.1: Covered threats and remaining risks acceptance

No.	Threat Actor	Threat action	Asset (relevant impact parameter)	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 connecte	d toy	Prevention: [ACM-FH] 5.6.1 [AUM-FH] 5.6.3 [AUTHZ-LP] 5.6.4 [AUTHZ-R] 5.6.5 [AUTHZ-PC] 5.6.6 [PRIV-FUNC-HIGH] 5.13.2 [LAS-PHY-INF] 5.12.3 [LAS-LOGIC-INF] 5.12.4 [LAS-APP] 5.12.5 [NOINF-AMP] 5.11.1 [PARCONT] 5.6.2 [SDC-AUM-FH] 5.4.1 [SDC-PARCONT] 5.4.5 Information: [MON-LOW] 5.14.1 [MON-MEDIUM] 5.14.2 [MON-HIGH] 5.14.3 [MON-HANDLE] 5.14.4 LOG-TIME] 5.14.5 [LOG-TIME-HIGH] 5.14.6 [LOG-STORE-MEDIUM] 5.14.7 [LOG-STORE-HIGH] 5.14.8 [LOG-CONFIG] 5.14.9 [SDC-MON-HANDLE] 5.4.6 [USERNOT-NOSECFUC] 5.2.1 Restoration: [SDC-FRM] 5.4.4	COM, IF and POE	C
[2]	A threat actor	tamper s	integrity relevant data	permane ntly stored on the internet connecte	d toy	Prevention: [PRIV-DATA-HIGH] 5.13.1 [INT-SSM] 5.8.1		C
[3]	A threat actor	tamper s	integrity relevant data	volatile stored on the internet connecte	d toy	Prevention: [PRIV-DATA-HIGH] 5.13.1		C

No.	Threat Actor	Threat action	Asset (relevant impact parameter)	Threat details		Requirement(s) for mitigation	Relevant attack surface parameter	Risk coverage
[4]	A threat actor	tamper s	integrity relevant data	communicated from or to the architectural component		Prevention: [INT-COM] 5.8.2	COM, IF and POE	C
[5]	A threat actor	discloses	confidential data	on the internet connected toy	unnecessarily processed	Prevention: [DMIN-DJST] 5.9.1		C
[6]	A threat actor	discloses	confidential data	permanently stored on the internet connected toy	during storage	Prevention: [CONF-SSM] 5.7.1 [PRIV-DATA-HIGH] 5.13.1	POE	C
[7]	A threat actor	discloses	confidential data	permanently stored on the internet connected toy	after deletion	Prevention: [DLM-PERM] 5.15.1		C
[8]	A threat actor	discloses	confidential data	volatile stored on the internet connected toy	during usage	Prevention: [PRIV-DATA-HIGH] 5.13.1		C
[9]	A threat actor	discloses	confidential data	volatile stored on the internet connected toy	after usage	Prevention: [PRIV-DATA-HIGH] 5.13.1		C
[10]	A threat actor	discloses	confidential data	communicated from or to the architectural component		Prevention: [CONF-COM] 5.7.2	COM, IF and POE	C
[12]	A threat actor	tamper s	integrity relevant function	on the internet connected toy		Prevention: [PRIV-DATA-HIGH] 5.13.1 [PRIV-FUNC-HIGH] 5.13.2 [INT-SWPCK] 5.8.3 [LAS-SBOOT] 5.12.6		C
[13]	A threat actor	impacts the availability of	time sensitive function	on the internet connected toy	by interruption caused by a software update installation	Prevention: [AVAI-SUM-SCHEDULE] 5.10.9		C

No.	Threat Actor	Threat action	Asset (relevant impact parameter)	Threat details		Requirement(s) for mitigation	Relevant attack surface parameter	Risk coverage
[14]	A threat actor	impacts the availability of	time sensitive function	on the internet connected toy	by interruption of power supply	Information: [AVAI-TIME-OUTA-NOT] 5.10.4 [AVAI-TIME-PREV-NOT] 5.10.5 Restoration: [AVAI-TIME-RECO-POW] 5.10.1		C
[15]	A threat actor	impacts the availability of	time sensitive function	on the internet connected toy	by interruption of network connection	Prevention: [AVAI-TIME-NETW] 5.10.2 Information: [AVAI-TIME-OUTA-NOT] 5.10.4 [AVAI-TIME-PREV-NOT] 5.10.5 Restoration: [AVAI-TIME-RECO-NETW] 5.10.3		C
[16]	A threat actor	impacts the availability of	time sensitive function	on the internet connected toy	due to overloading of a resource or connection	Prevention: [AVAI-TIME-NET-PRIO] 5.10.6 [AVAI-TIME-RES-PRIO] 5.10.7 [AVAI-TIME-DOS-RATE] 5.10.8 Information: [AVAI-TIME-OUTA-NOT] 5.10.4	IF	C
[17]	A threat actor	exploits an implementation vulnerability to compromise	a product cybersecurity asset			Prevention: [PRIV-DATA-HIGH] 5.13.1 [PRIV-FUNC-HIGH] 5.13.2 [LAS-INVAL] 5.12.1 [LAS-INSAN] 5.12.2 [NKEV-MKAV] 5.3.1 Information: [NKEV-INIT-UDP] 5.3.2 [SDC-SUM-NOTIF] 5.4.3 [SU-DISABLE-AUTO] 5.5.4 [SU-POSTPONE-AUTO] 5.5.5 [SU-NOTIF] 5.5.6 Restoration: [NKEV-INIT-UDP] 5.3.2 [SDC-SUM-AUTO] 5.4.2 [SU-SUPPORT] 5.5.1 [SU-PROVIDE] 5.5.2 [SU-AUTO] 5.5.3		C
[18]	A user	unconsciously performs an incorrect actions		on the internet connected toy		Prevention: [GUI-SECCONF] 5.2.3 Information: [GUI-SECCONF] 5.2.3	IF.Human	C
[19]	A user	performs insecure actions		on the internet connected toy	because the user is not aware of security relevant information	Prevention: [USERNOT-SECREL] 5.2.2 Information: [USERNOT-SECREL] 5.2.2	IF.Human	C

No.	Threat Actor	Threat action	Asset (relevant impact parameter)	Threat details		Requirement(s) for mitigation	Relevant attack surface parameter	Risk coverage
[20]	An incident	results in a permanent loss of	loss sensitive data	permanently stored on the internet connected toy		Prevention: [BACKUP-TRANS] 5.2.4 [BACKUP-AUTOTRANS] 5.2.5 [BACKUP-EXPORT] 5.2.6		C

- The columns *Threat Actor*, *Threat Action*, *Asset*, and *Threat Details* describe the threat scenario under consideration.
- The column *Asset* describes the asset affected by this threat scenario and indicates, where relevant, the corresponding impact parameter (e.g. [IMP.FH] is the relevant impact parameter for threats addressing function, whose use can cause harm).
- The column *Requirement(s) for mitigation* refers to the mitigations of the risks that arise from the threat scenario.
- The *Relevant attack surface parameter* column describes which of the attack surface parameters make a difference in mitigation.
- 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).

B.7 Guidance for determining impact classes

B.7.1 General

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

B.7.2 Confidential data

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

The disclosure may lead to:

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

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

The disclosure may lead to:

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

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

The disclosure may lead to:

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

B.7.3 Loss sensitive data

loss sensitive availability impact class low (IMP.AVALOSS.Low):

The loss may lead to:

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

loss sensitive availability impact class medium (IMP.AVALOSS.Medium):

The loss may lead to:

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

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

The loss may lead to:

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

B.7.4 Time sensitive function

time sensitive availability impact class low (IMP.AVALTIME.Low):

The delay of availability may lead to:

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

time sensitive availability impact class medium (IMP.AVALTIME.Medium):

The delay of availability may lead to:

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

time sensitive availability impact class high (IMP.AVALTIME.High):

The delay of availability may lead to:

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

B.7.5 Integrity relevant data and integrity relevant function

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

The tampering may lead to:

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

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

The tampering may lead to:

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

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

The tampering may lead to:

- significant or even irreversible impact on the user(s) (e.g. personal or financial harm);
- additional or increased attack opportunities for a prolonged time on the internet connected toy or a limited number of other products;
- additional or increased attack opportunities for a short time on a significant number of other products;
- non-availability of key-functionalities of the internet connected toy for a prolonged time; or
- permanent non-availability of non-key-functionalities of the internet connected toy.

Annex C:
Void

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

D.1 Data assets

The impact classes shall be assigned to data assets in accordance with table [D.1](#).

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 loss critical availability relevant internet connected toy data
Activity data	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
Audit event data	IMP.CONF = Maximum(IMP.CONF of confidential data contained in the audit event data)	IMP.INT = Maximum(IMP.FH of internet connected toys functions using audit event data)	IMP.AVAI.LOSS.MEDIUM
Authorisation policy data	IMP.CONF.MEDIUM	IMP.INT.HIGH	IMP.AVAI.LOSS.LOW
Cryptographic security parameter	IMP.CONF = Maximum(Maximum(IMP.C ONF, IMP.INT of all data assets whose protection relies on the confidentiality of the cryptographic security parameter),Maximum(IMP.I NT, IMP.FH of all function assets whose protection relies on the confidentiality of the cryptographic security parameter))	IMP.INT = Maximum(Maximum(IMP.C ONF, IMP.INT of all data assets whose protection relies on the integrity of the cryptographic security parameter),Maximum(IMP.I NT, IMP.FH of all function assets whose protection relies on the integrity 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)
Device identifier data	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.LOW
Entity's location data	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
Function binary data	NO	IMP.INT = Maximum(IMP.FH, IMP.INT, IMP.AVAI.TIME of function it implements)	NO
Function configuration data	NO	IMP.INT = Maximum(IMP.INT, IMP.AVAI.TIME, IMP.FH of configured function)	IMP.AVAI.LOSS = Maximum(IMP.AVAI.TIME of configured function)
Identity data for authentication	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.LOW
Logging data	IMP.CONF = Maximum(IMP.CONF of confidential data contained in the logging data)	IMP.INT = Maximum(IMP.FH of internet connected toys functions using logging data)	IMP.AVAI.LOSS.MEDIUM
Network status data	IMP.CONF.LOW	IMP.INT.MEDIUM	IMP.AVAI.LOSS.LOW
Personal contact data	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
Personal notes data	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
Private audio data	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM

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 loss critical availability relevant internet connected toy data
Private video data	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
Public data asset	IMP.CONF.LOW	IMP.INT.MEDIUM	NO
Real-time data	NO	IMP.INT.MEDIUM	NO
Social interactive data	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.LOW
Software package	IMP.CONF = Maximum(IMP.CONF of confidential data contained in the package)	IMP.INT = Maximum(IMP.INT of internet connected toy's integrity relevant function)	NO
State data	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.LOW

D.2 Function assets

The impact classes shall be assigned to function assets in accordance with tables [D.2](#) and [D.3](#).

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
Connection function	IMP.INT.LOW	IMP.AVAI.TIME.LOW	IMP.FH.MEDIUM
Data presenting function	IMP.INT = Maximum(IMP.CONF, IMP.INT of communicated data)	NO	IMP.FH = Maximum(LOW,Maximum(I MP.CONF of communicated data)
External sensing function	IMP.INT = Maximum(IMP.INT of modified data)	NO	IMP.FH = Maximum(IMP.INT of modified data)
Internal sensing function	IMP.INT = Maximum(IMP.CONF, IMP.INT of presented data)	NO	IMP.FH = Maximum(IMP.CONF of presented data)
Internet connected toy function which can communicate internet connected toy data	IMP.INT = Maximum(IMP.INT of measured data)	NO	IMP.FH = Maximum(IMP.CONF, IMP.INT of measured data)
Internet connected toy function which can modify internet connected toy data	IMP.INT = Maximum(IMP.INT of measured data)	NO	IMP.FH = Maximum(IMP.CONF, IMP.INT of measured data)
Parental control function	IMP.INT.MEDIUM	IMP.AVAI.TIME.LOW	IMP.FH.MEDIUM
Security function	IMP.INT = Maximum(Maximum(IMP.IN T of protected data),Maximum(IMP.INT of protected functions))	IMP.AVAI.TIME = Maximum(IMP.AVAI.TIME of protected functions)	NO

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](#).

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
Connection function	NO	IMP.FH.DSN.MEDIUM	NO	NO
Data presenting function	NO	IMP.FH.DSN.LOW	IMP.FH.CCON = Maximum(IMP.CONF of communicated data)	NO
External sensing function	NO	NO	NO	IMP.FH.MINT = Maximum(IMP.INT of modified data)
Internal sensing function	IMP.FH.SP = Maximum(IMP.CONF of presented data)	NO	IMP.FH.CCON = Maximum(IMP.CONF of presented data)	NO
Internet connected toy function which can communicate internet connected toy data	IMP.FH.SP = Maximum(IMP.CONF of measured data)	NO	NO	IMP.FH.MINT = Maximum(IMP.INT of measured data)
Internet connected toy function which can modify internet connected toy data	IMP.FH.SP = Maximum(IMP.CONF of measured data)	NO	NO	IMP.FH.MINT = Maximum(IMP.INT of measured data)
Parental control function	NO	NO	IMP.FH.CCON.LOW	IMP.FH.MINT.MEDIUM
Security function	NO	NO	NO	NO

Annex E (normative): Protection measures

E.1 Authentication mechanism strength

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

E.1.1.1 General

Specific requirements on authentication mechanisms for the AUTH strength level determined in clause 5.6.3. Note that for AUTH.Normal, AUTH.Enhanced and AUTH.Strong, the requirements in clause E.1.1.5 and clause E.1.1.6 are also to be considered.

E.1.1.2 [AUM-E-I-Basic] AUTH.Basic inference based SFA

Where an authentication factor of the type inference is used to achieve AUTH.Basic, the authentication mechanisms shall ensure a false acceptance rate of maximal 10^{-4} and a false rejection rate of maximal 10^{-1} .

NOTE: The values used for false acceptance rate and false rejection rate are based on ETSI TS 103 732-2 [i.8].

E.1.1.3 [AUM-E-K-Basic] AUTH.Basic knowledge based SFA

Where an authentication factor of the type knowledge is used to achieve AUTH.Basic, the authentication mechanisms shall ensure a security insurance time of one day (86 400 s) with a probability of guessing a cryptographic parameter of maximal 10^{-2} .

NOTE: The p_{GRP} allows for a tradeoff between complexity of passwords or PINs and restrictions on the number of attempts to enter a password or PIN.

E.1.1.4 [AUM-E-I-Normal] AUTH.Normal inference based SFA

Where an authentication factor of the type inference is used to achieve AUTH.Normal, the authentication mechanisms shall ensure a false acceptance rate of maximal 5×10^{-5} and a false rejection rate of maximal 10^{-1} .

NOTE: The values used for false acceptance rate and false rejection rate are based on ETSI TS 103 732-2 [i.8].

E.1.1.5 [AUM-E-K-Normal] AUTH.Normal knowledge based SFA

Where an authentication factor of the type knowledge is used to achieve AUTH.Enhanced, the authentication mechanisms shall ensure a security insurance time of one month ($2,6 \times 10^6$ s) with a cryptographic parameter guessing probability of maximal 10^{-3} .

NOTE: The p_{GRP} allows for a tradeoff between complexity of passwords or PINs and restrictions on the number of attempts to enter a password or PIN.

E.1.1.6 [AUM-E-P-Normal] AUTH.Normal possession based SFA

Where an Account or Service is used as an possession type authentication factor to achieve AUTH.Normal, the authentication mechanisms shall ensure that:

- derived tokens have a time during which a token is valid of maximal 15 minutes (900 s); and

- all derived tokens that can be valid at the same time have a combined cryptographic parameter guessing probability of maximal 10^{-3} within the time during which a token is valid.

NOTE 1: The p_{GRP} allows for a tradeoff between complexity of passwords or PINs and restrictions on the number of attempts to enter a password or PIN.

NOTE 2: The calculation of $L_{CP,eff}$ is based on the recommendations in NIST SP 800-78-5 [i.9].

E.1.1.7 [AUM-E-MFA-Normal] AUTH.Normal MFA

Where multiple authentication factors are used to achieve AUTH.Normal, the authentication mechanism shall ensure that:

- at least two authentication factors are of different types (inherence, knowledge or possession); and
- it fulfils the respective SFA requirements of at least AUTH.Basic with at least these two authentication factors; and
- that the authentication request is only considered valid if at least these two authentication factors are validated within maximal 30 minutes (1 800 s) of each other.

E.1.1.8 [AUM-E-I-Enhanced] AUTH.Enhanced inherence based SFA

Where an authentication factor of the type inherence is used to achieve AUTH.Basic, the authentication mechanisms shall ensure a false acceptance rate of maximal 5×10^{-5} and a false rejection rate of maximal 3×10^{-2} .

NOTE: The values used for false acceptance rate and false rejection rate are based on ETSI TS 103 732-2 [i.8].

E.1.1.9 [AUM-E-K-Enhanced] AUTH.Enhanced knowledge based SFA

Where an authentication factor of the type knowledge is used to achieve AUTH.Normal, the authentication mechanisms shall ensure a security insurance time of one year ($3,2 \times 10^7$ s) with a cryptographic parameter guessing probability of maximal 10^{-5} .

NOTE: The p_{GRP} allows for a tradeoff between complexity of passwords or PINs and restrictions on the number of attempts to enter a password or PIN.

E.1.1.10 [AUM-E-P-Enhanced] AUTH.Enhanced possession based SFA

Where an Account or Service or security token is used as an possession type authentication factor to achieve AUTH.Enhanced, the authentication mechanisms shall ensure that:

- confidential cryptographic keys in security tokens have a effective cryptographic security parameter bitlength of minimal 125 bit; and
- derived tokens have a time during which a token is valid of maximal 10 minutes (600 s); and
- all derived tokens that can be valid at the same time have a combined cryptographic parameter guessing probability of maximal 10^{-5} within the time during which a token is valid.

NOTE 1: The p_{GRP} allows for a tradeoff between complexity of passwords or PINs and restrictions on the number of attempts to enter a password or PIN.

NOTE 2: The calculation of $L_{CP,eff}$ is based on the recommendations in NIST SP 800-78-5 [i.9].

E.1.1.11 [AUM-E-MFA-Enhanced] AUTH.Enhanced MFA

Where multiple authentication factors are used to achieve AUTH.Enhanced, the authentication mechanism shall ensure that:

- at least two authentication factors are of different types (inherence, knowledge or possession); and

- it fulfils the respective SFA requirements of at least AUTH.Normal with at least these two authentication factors; and
- that the authentication request is only considered valid if at least these two authentication factors are validated within maximal 15 minutes (900 s) of each other.

E.1.1.12 [AUM-E-I-Strong] AUTH.Strong inheritance based SFA

Where an authentication factor of the type inheritance is used to achieve AUTH.Strong, the authentication mechanisms shall ensure a false acceptance rate of maximal 10^{-5} and a false rejection rate of maximal 3×10^{-2} .

NOTE: The values used for false acceptance rate and false rejection rate are based on ETSI TS 103 732-2 [i.8].

E.1.1.13 [AUM-E-P-Strong] AUTH.Strong possession based SFA

Where a security token is used as an possession type authentication factor to achieve AUTH.Strong, the authentication mechanisms shall ensure that:

- confidential cryptographic keys cannot be extracted from a security token; and
- confidential cryptographic keys in security tokens have a effective cryptographic security parameter bitlength of minimal 125 bit; and
- derived tokens have a time during which a token is valid of maximal five minutes (300 s); and
- all derived tokens that can be valid at the same time have a combined cryptographic parameter guessing probability of maximal 10^{-6} within the time during which a token is valid.

NOTE 1: The p_{GRP} allows for a tradeoff between complexity of passwords or PINs and restrictions on the number of attempts to enter a password or PIN.

NOTE 2: The calculation of $L_{CP,eff}$ is based on the recommendations in NIST SP 800-78-5 [i.9].

E.1.1.14 [AUM-E-MFA-Strong] AUTH.Strong MFA

Where multiple authentication factors are used to achieve AUTH.Strong, the authentication mechanism shall ensure that:

- at least two authentication factors are of different types (inheritance, knowledge or possession); and
- it fulfils the respective SFA requirements of at least AUTH.Enhanced with all of these authentication factors; and
- that the authentication request is only considered valid if all of these authentication factors are validated within maximal 10 minutes of each other.

E.1.1.15 [AUM-E-Replay] AUTH.Normal, AUTH.Enhanced and AUTH.Strong replay protection

Where authentication mechanisms are accessible via interfaces with local communication, adjacent communication or public communication and provide AUTH.Normal, AUTH.Enhanced or AUTH.Strong, the authentication mechanisms shall protect against authentication of a third entity (attacker) by interception and retransmission of valid transmissions between the internet connected toy and another entity.

E.1.1.16 [AUM-E-PitM] AUTH.Normal, AUTH.Enhanced and AUTH.Strong person in the middle protection

Where authentication mechanisms are accessible via interfaces with local communication, adjacent communication or public communication and provide AUTH.Normal, AUTH.Enhanced or AUTH.Strong, the authentication mechanisms shall protect against authentication of a third entity (attacker) by interception and alteration of data transmissions between the internet connected toy and the entity that requests authentication.

E.1.2 Assessment for [AUM-FH] authentication mechanism strength

E.1.2.1 General

Specific assessments on authentication mechanisms for the AUTH strength level determined in clause [5.6.3](#).

E.1.2.2 Assessment criteria for [AUM-E-I-Basic]

Assessment reference:

[\[AUM-E-I-Basic\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the internet connected toy to fulfil [AUM-FH] clause [5.6.3](#) for authentication level AUTH.Basic using inherence authentication factors,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the authentication mechanism used by the internet connected toy to achieve AUTH.Basic using inherence authentication factors:
 - documentation of the authentication factors that can be used.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Basic is created;
- a test setup to access the documented authentication mechanism via a documented interface.

Assessment activities:

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces; and
- determine the FAR value of the authentication mechanism;
- determine the FRR value of the authentication mechanism.

Assessment verdict:

The verdict PASS shall be assigned if:

- the authentication mechanism used to achieve AUTH.Basic with inherence authentication factors has a FAR of maximal 10^{-4} ; and

- the authentication mechanism used to achieve AUTH.Basic with inherence authentication factors has a FRR of maximal 10^{-1} ; and
- there is no indication, that the authentication mechanism used to achieve AUTH.Basic with inherence authentication factors differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.1.2.3 Assessment criteria for [AUM-E-K-Basic]

Assessment reference:

[\[AUM-E-K-Basic\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the internet connected toy to fulfil [AUM-FH] clause [5.6.3](#) for authentication level AUTH.Basic using knowledge authentication factors.

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the authentication mechanism used by the internet connected toy to achieve AUTH.Basic using knowledge authentication factors:
 - documentation of the authentication factors that can be used

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Basic is created;
- a test setup to access the documented authentication mechanism via a documented interface.

Assessment activities:

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- determine the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) value of the authentication mechanism;
- determine the maximum sustained validation attempt frequency ($f_{VA,max}$) value of the authentication mechanism;
- calculate the cryptographic parameter guessing probability (p_{GRP}) for a security insurance time (security insurance time) of one day $p_{GRP} = T_{SI} * f_{VA,max}$ / **Assessment verdict:**

The verdict PASS shall be assigned if:

- the authentication mechanism used to achieve AUTH.Basic with knowledge authentication factors have a p_{GRP} of maximal 10^{-2} for a T_{SI} of one day; and
- there is no indication, that the authentication mechanism used to achieve AUTH.Basic with knowledge authentication factors differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.1.2.4 Assessment criteria for [AUM-E-I-Normal]**Assessment reference:**

[\[AUM-E-I-Normal\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the internet connected toy to fulfil [AUM-FH] clause [5.6.3](#) for authentication level AUTH.Normal using inherence authentication factors,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the authentication mechanism used by the internet connected toy to achieve AUTH.Normal using inherence authentication factors:
 - documentation of the authentication factors that can be used.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Normal is created;
- a test setup to access the documented authentication mechanism via a documented interface.

Assessment activities:

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- determine the FAR value of the authentication mechanism;
- determine the FRR value of the authentication mechanism.

Assessment verdict:

The verdict PASS shall be assigned if:

- the authentication mechanism used to achieve AUTH.Normal with inherence authentication factors has a FAR of maximal 5×10^{-5} ; and
- the authentication mechanism used to achieve AUTH.Normal with inherence authentication factors has a FRR of maximal 10^{-1} ; and
- there is no indication, that an authentication mechanisms used to achieve AUTH.Normal with inherence authentication factors differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.1.2.5 Assessment criteria for [AUM-E-K-Normal]

Assessment reference:

[\[AUM-E-K-Normal\]](#)

Assessment objective:

The assessment covers:

a functional sufficiency assessment of an authentication mechanism used by the internet connected toy to fulfil [AUM-FH] clause [5.6.3](#) for authentication level AUTH.Normal using knowledge authentication factors, based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the authentication mechanism used by the internet connected toy to achieve AUTH.Normal using knowledge authentication factors:
 - documentation of the authentication factors that can be used.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Normal is created;
- a test setup to access the documented authentication mechanism via a documented interface.

Assessment activities:

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- determine the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) value of the authentication mechanism;
- determine the maximum sustained validation attempt frequency ($f_{VA,max}$) value of the authentication mechanism;
- calculate the cryptographic parameter guessing probability (p_{GRP}) for a security insurance time (T_{SI}) of one month ($2,6 \times 10^6$ s) $p_{GRP} = T_{SI} * f_{VA,max} / C_{CP,min}$.

Assessment verdict:

The verdict PASS shall be assigned if:

- the authentication mechanism used to achieve AUTH.Normal with knowledge authentication factors have a p_{GRP} of maximal 10^{-3} for a T_{SI} of one month; and
- there is no indication, that the authentication mechanism used to achieve AUTH.Normal with knowledge authentication factors differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.1.2.6 Assessment criteria for [AUM-E-P-Normal]

Assessment reference:

[\[AUM-E-P-Normal\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the internet connected toy to fulfil [AUM-FH] clause [5.6.3](#) for authentication level AUTH.Normal using possession authentication factors based on Accounts or Services,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the authentication mechanism used by the internet connected toy to achieve AUTH.Normal using possession authentication factors based on Accounts or Services:
 - documentation of Accounts or Services that can be used by the authentication mechanism;
 - documentation of how a security tokens authenticity is validated by the authentication mechanism.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Normal is created;
- a suitable security token is known to the authentication mechanism;
- a test setup to access the documented authentication mechanism via a documented interface.

Assessment activities:

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- where derived tokens are used to validate the authenticity of a security token:
 - determine the time during which a token is valid (T_{VA}) of the authentication mechanism for these derived tokens;
 - determine the maximal valid derived tokens ($n_{dt,max}$);
 - determine the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) value of the authentication mechanism;
 - determine the maximum sustained validation attempt frequency ($f_{VA,max}$) value of the authentication mechanism;
 - calculate the combined cryptographic parameter guessing probability (p_{GRP}) for the derived tokens, that can be valid at the same time: $p_{GRP} = T_{VA} * f_{VA,max} * n_{dt,max} / C_{CP,min}$.

Assessment verdict:

The verdict PASS shall be assigned if:

- derived tokens have a time during which a token is valid of maximal 15 minutes (900 s); and
- derived tokens have a combined cryptographic parameter guessing probability of maximal 10^{-3} ; and
- there is no indication, that the authentication mechanisms used to achieve AUTH.Normal with possession authentication factor differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.1.2.7 Assessment criteria for [AUM-E-MFA-Normal]

Assessment reference:

[\[AUM-E-MFA-Normal\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the internet connected toy to fulfil [AUM-FH] clause [5.6.3](#) for authentication level AUTH.Normal using MFA,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the authentication mechanism used by the internet connected toy to achieve AUTH.Normal using MFA:
 - documentation of the authentication factors that can be used.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Normal is created;
- a test setup to access the documented authentication mechanism via a documented interface.

Assessment activities:

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- verify whether authentication factors of the same type can be used for MFA;
- for authentication factors based on knowledge, verify whether the authentication mechanism would satisfy the assessment clause [E.1.2.3](#) (or clause [E.1.2.5](#), clause [E.1.2.9](#));
- for authentication factors based on inherence, verify whether the authentication mechanism would satisfy the assessment clause [E.1.2.2](#) (or clause [E.1.2.4](#), clause [E.1.2.8](#), clause [E.1.2.2](#));
- for authentication factors based on possession, verify whether the authentication mechanism would satisfy the assessment clause [E.1.2.6](#) (or clause [E.1.2.0](#), clause [E.1.2.3](#));
- determine the maximal time between entering the first and the last authentication factor for an authentication attempt to be successful.

Assessment verdict:

The verdict PASS shall be assigned if:

- at least two authentication factors are of different types are necessary for a successful authentication; and
- satisfies the assessment for AUTH.Normal or higher with at least these two authentication factors; and
- at least these two authentication factors have to be validated within maximal 15 minutes (900 s) of each other for a successful authentication; and
- there is no indication, that the authentication mechanism used to achieve AUTH.Normal with MFA differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.1.2.8 Assessment criteria for [AUM-E-I-Enhanced]**Assessment reference:**

[\[AUM-E-I-Enhanced\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the internet connected toy to fulfil [AUM-FH] clause [5.6.3](#) for authentication level AUTH.Enhanced using inherence authentication factors,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the authentication mechanism used by the internet connected toy to achieve AUTH.Enhanced using inherence authentication factors:
 - documentation of the authentication factors that can be used.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Enhanced is created;
- a test setup to access the documented authentication mechanism via a documented interface.

Assessment activities:

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- determine the FAR value of the authentication mechanism;
- determine the FRR value of the authentication mechanism.

Assessment verdict:

The verdict PASS shall be assigned if:

- the authentication mechanism used to achieve AUTH.Enhanced with inherence authentication factors has a FAR of maximal 5×10^{-5} ; and
- the authentication mechanism used to achieve AUTH.Enhanced with inherence authentication factors has a FRR of maximal 3×10^{-2} ; and
- there is no indication, that the authentication mechanism used to achieve AUTH.Enhanced with inherence authentication factors differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.1.2.9 Assessment criteria for [AUM-E-K-Enhanced]

Assessment reference:

[\[AUM-E-K-Enhanced\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the internet connected toy to fulfil [AUM-FH] clause [5.6.3](#) for authentication level AUTH.Enhanced using knowledge authentication factors,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the authentication mechanism used by the internet connected toy to achieve AUTH.Enhanced using knowledge authentication factors:
 - documentation of the authentication factors that can be used.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Enhanced is created;
- a test setup to access the documented authentication mechanism via a documented interface.

Assessment activities:

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- determine the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) value of the authentication mechanism;
- determine the maximum sustained validation attempt frequency ($f_{VA,max}$) value of the authentication mechanism;
- calculate the cryptographic parameter guessing probability (p_{GRP}) for a security insurance time (T_{SI}) of one year ($3,2 \times 10^7$ s) $p_{GRP} = T_{SI} * f_{VA,max} / C_{CP,min}$.

Assessment verdict:

The verdict PASS shall be assigned if:

- the authentication mechanism used to achieve AUTH.Enhanced with knowledge authentication factors have a p_{GRP} of maximal 10^{-5} for a T_{SI} of one year; and
- there is no indication, that the authentication mechanism used to achieve AUTH.Enhanced with knowledge authentication factors differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.1.2.10 Assessment criteria for [AUM-E-P-Enhanced]

Where an Account or Service is used as an authentication factor of the type possession for authentication level AUTH.Enhanced, the following assessment has to be performed:

Assessment reference:

[\[AUM-E-P-Enhanced\]](#) for accounts or services used as an authentication factor.

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the internet connected toy to fulfil [AUM-FH] clause [5.6.3](#) for authentication level AUTH.Enhanced using possession authentication factors based on Accounts or Services.

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the authentication mechanism used by the internet connected toy to achieve AUTH.Enhanced using possession authentication factors based on Accounts or Services:
 - documentation of Accounts or Services that can be used by the authentication mechanism;
 - documentation of how a security tokens authenticity is validated by the authentication mechanism.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Enhanced is created;
- a suitable security token is known to the authentication mechanism;
- a test setup to access the documented authentication mechanism via a documented interface.

Assessment activities:

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- where derived tokens are used to validate the authenticity of a security token:
 - determine the time during which a token is valid (T_{VA}) of the authentication mechanism for these derived tokens;
 - determine the maximal valid derived tokens ($n_{dt,max}$); and
 - determine the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) value of the authentication mechanism;
 - determine the maximum sustained validation attempt frequency ($f_{VA,max}$) value of the authentication mechanism;
 - calculate the combined cryptographic parameter guessing probability (p_{GRP}) for the derived tokens, that can be valid at the same time: $p_{GRP} = T_{VA} * f_{VA,max} * n_{dt,max} / C_{CP,min}$.

Assessment verdict:

The verdict PASS shall be assigned if:

- derived tokens have a time during which a token is valid of maximal 10 minutes; and
- derived tokens have a combined cryptographic parameter guessing probability of maximal 10^{-4} ; and

- there is no indication, that the authentication mechanism used to achieve AUTH.Enhanced with possession authentication factor differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

Where a security token is used as an authentication factor of the type possession for authentication level AUTH.Enhanced, the following assessment has to be performed:

Assessment reference:

[\[AUM-E-P-Enhanced\]](#) for a security token used as an authentication factor

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the internet connected toy to fulfil [AUM-FH] clause [5.6.3](#) for authentication level AUTH.Enhanced using possession authentication factors based on security tokens,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the authentication mechanism used by the internet connected toy to achieve AUTH.Enhanced using possession authentication factors based on security tokens:
 - documentation of security tokens that can be used by the authentication mechanism.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Enhanced is created;
- suitable security tokens for the documented authentication mechanisms;
- a test setup to access the documented authentication mechanism via a documented interface.

Assessment activities:

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- determine the minimal effective cryptographic security parameter bitlength of the security tokens that can be used by the authentication mechanism;
- where derived tokens are used to validate the authenticity of a security token:
 - determine the time during which a token is valid (T_{VA}) of the authentication mechanism for derived tokens;
 - determine the maximal valid derived tokens ($n_{dt,max}$); and
 - determine the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) value of the derived tokens;
 - determine the maximum sustained validation attempt frequency ($f_{VA,max}$) value of the authentication mechanism; and
 - calculate the combined cryptographic parameter guessing probability (p_{GRP}) for the derived tokens, that can be valid at the same time: $p_{GRP} = T_{VA} * f_{VA,max} * n_{dt,max} / C_{CP,min}$.

Assessment verdict:

The verdict PASS shall be assigned if:

- security tokens have a effective cryptographic security parameter bitlength of minimal 125 bit; and
- derived tokens have a time during which a token is valid of maximal 10 minutes; and
- derived tokens have a combined cryptographic parameter guessing probability of maximal 10^{-5} ; and
- there is no indication, that the authentication mechanism used to achieve AUTH.Enhanced with possession authentication factor differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.1.2.11 Assessment criteria for [AUM-E-MFA-Enhanced]**Assessment reference:**

[\[AUM-E-MFA-Enhanced\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the internet connected toy to fulfil [AUM-FH] clause [5.6.3](#) for authentication level AUTH.Enhanced using MFA,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the authentication mechanism used by the internet connected toy to achieve AUTH.Enhanced using MFA:
 - documentation of the authentication factors that can be used.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Enhanced is created;
- a test setup to access the documented authentication mechanism via a documented interface.

Assessment activities:

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- verify whether authentication factors of the same type can be used for MFA;
- for authentication factors based on knowledge, verify whether the authentication mechanism would satisfy the assessment clause [E.1.2.5](#) (or clause [E.1.2.9](#));
- for authentication factors based on inherence, verify whether the authentication mechanism would satisfy the assessment clause [E.1.2.4](#) (or clause [E.1.2.8](#), clause [E.1.2.2](#));
- for authentication factors based on possession, verify whether the authentication mechanism would satisfy the assessment clause [E.1.2.6](#) (or clause [E.1.2.0](#), clause [E.1.2.3](#));

- determine the maximal time between entering the first and the last authentication factor for an authentication attempt to be successful.

Assessment verdict:

The verdict PASS shall be assigned if:

- at least two authentication factors are of different types are necessary for a successful authentication; and
- satisfies the assessment for AUTH.Normal or higher with at least these two authentication factors; and
- at least these two authentication factors have to be validated within maximal 10 minutes (600 s) of each other for a successful authentication; and
- there is no indication, that the authentication mechanism used to achieve AUTH.Enhanced with MFA differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.1.2.12 Assessment criteria for [AUM-E-I-Strong]

Assessment reference:

[\[AUM-E-I-Strong\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the internet connected toy to fulfil [AUM-FH] clause [5.6.3](#) for authentication level AUTH.Strong using inherence authentication factors,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the authentication mechanism used by the internet connected toy to achieve AUTH.Strong using inherence authentication factors:
 - documentation of the authentication factors that can be used.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Strong is created;
- a test setup to access the documented authentication mechanism via a documented interface.

Assessment activities:

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- determine the FAR value of the authentication mechanism;
- determine the FRR value of the authentication mechanism.

Assessment verdict:

The verdict PASS shall be assigned if:

- the authentication mechanism used to achieve AUTH.Strong with inherence authentication factors has a FAR of maximal 10^{-5} ; and
- the authentication mechanism used to achieve AUTH.Strong with inherence authentication factors has a FRR of maximal 3×10^{-2} ; and
- there is no indication, that the authentication mechanism used to achieve AUTH.Strong with inherence authentication factors differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.1.2.13 Assessment criteria for [AUM-E-P-Strong]

Assessment reference:

[\[AUM-E-P-Strong\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the internet connected toy to fulfil [AUM-FH] clause [5.6.3](#) for authentication level AUTH.Strong using possession authentication factors based on security tokens,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the authentication mechanism used by the internet connected toy to achieve AUTH.Strong using possession authentication factors based on security tokens:
 - documentation of security tokens that can be used by the authentication mechanism.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Strong is created;
- suitable security tokens for the documented authentication mechanisms;
- a test setup to access the documented authentication mechanism via a documented interface.

Assessment activities:

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- determine the minimal effective cryptographic security parameter bitlength of the security tokens that can be used by the authentication mechanism;
- where derived tokens are used to validate the authenticity of a security token:
 - determine the time during which a token is valid (T_{VA}) of the authentication mechanism for derived tokens;

- determine the maximal valid derived tokens ($n_{dt,max}$); and
- determine the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) value of the derived tokens;
- determine the maximum sustained validation attempt frequency ($f_{VA,max}$) value of the authentication mechanism;
- calculate the combined cryptographic parameter guessing probability (p_{GRP}) for the derived tokens, that can be valid at the same time: $p_{GRP} = T_{VA} * f_{VA,max} * n_{dt,max} / C_{CP,min}$.

Assessment verdict:

The verdict PASS shall be assigned if:

- security tokens have a effective cryptographic security parameter bitlength of minimal 125 bit; and
- derived tokens have a time during which a token is valid of maximal five minutes; and
- derived tokens have a combined cryptographic parameter guessing probability of maximal 10^{-4} ; and
- there is no indication, that an authentication mechanisms used to achieve AUTH.Strong with possession authentication factor differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.1.2.14 Assessment criteria for [AUM-E-MFA-Strong]

Assessment reference:

[\[AUM-E-MFA-Strong\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the internet connected toy to fulfil [AUM-FH] clause [5.6.3](#) for authentication level AUTH.Strong using MFA,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the authentication mechanism used by the internet connected toy to achieve AUTH.Strong using MFA;
 - documentation of the authentication factors that can be used.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Strong is created;
- a test setup to access the documented authentication mechanism via a documented interface.

Assessment activities:

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- verify whether authentication factors of the same type can be used for MFA;

- for authentication factors based on knowledge, verify whether the authentication mechanism would satisfy the assessment clause [E.1.2.9](#);
- for authentication factors based on inherence, verify whether the authentication mechanism would satisfy the assessment clause [E.1.2.8](#) (or clause [E.1.2.2](#));
- for authentication factors based on possession, verify whether the authentication mechanism would satisfy the assessment clause [E.1.2.0](#) (or clause [E.1.2.3](#));
- determine the maximal time between entering the first and the last authentication factor for an authentication attempt to be successful.

Assessment verdict:

The verdict PASS shall be assigned if:

- at least two authentication factors are of different types are necessary for a successful authentication; and
- satisfies the assessment for AUTH.Normal or higher with all of these authentication factors; and
- all of these authentication factors have to be validated within 5 minutes (300 s) of each other for a successful authentication; and
- there is no indication, that the authentication mechanism used to achieve AUTH.Strong with MFA differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.1.2.15 Assessment criteria for [AUM-E-Replay]

Assessment reference:

[\[AUM-E-Replay\]](#)

Assessment objective:

The assessment covers:

- a functional assessment of authentication mechanisms that are accessible via interfaces with local communication, adjacent communication or public communication and provide AUTH.Normal, AUTH.Enhanced or AUTH.Strong.

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the authentication mechanism that are accessible via interfaces with local communication, adjacent communication or public communication and provide AUTH.Normal, AUTH.Enhanced or AUTH.Strong:
 - documentation of the communication protocols uses for the authentication process.

The following test setups shall be prepared:

- a communication partner with active authentication mechanisms shall be set up for the internet connected toy;
- a capture and replay tool between internet connected toy and its communication partner shall be set up;
- at least one interface, where the authentication mechanism is reachable shall be documented.

Assessment activities:

The following activities shall be performed:

- authentication mechanisms that are accessible via interfaces with local communication, adjacent communication or public communication and provide AUTH.Normal, AUTH.Enhanced or AUTH.Strong:
 - initiate a connection between the internet connected toy and its communication partner;
 - use a capture tool to record the transmitted message or transaction data;
 - replay (retransmit) the captured message to the authentication mechanism using a suitable tool in place to mimic the original communication partner;
 - record if the authentication mechanism accepts the retransmitted data.

Assessment verdict:

The verdict PASS shall be assigned if:

- the authentication mechanism does not accept the retransmitted data as valid authentication attempts.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- description of the performed test;
- all test records of the performed test.

E.1.2.16 Assessment criteria for [AUM-E-PitM]

Assessment reference:

[\[AUM-E-PitM\]](#)

Assessment objective:

The assessment covers:

- a functional assessment of authentication mechanisms that are accessible via interfaces with local communication, adjacent communication or public communication and provide AUTH.Normal, AUTH.Enhanced or AUTH.Strong,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the authentication mechanism that are accessible via interfaces with local communication, adjacent communication or public communication and provide AUTH.Normal, AUTH.Enhanced or AUTH.Strong:
 - documentation of the communication protocols used for the authentication process.

The following test setups shall be prepared:

- a communication partner with active authentication mechanisms shall be set up for the internet connected toy;
- a capture and PitM tool between internet connected toy and its communication partner shall be set up;
- at least one interface, where the authentication mechanism is reachable shall be documented.

Assessment activities:

The following activities shall be performed:

- authentication mechanisms that are accessible via interfaces with local communication, adjacent communication or public communication and provide AUTH.Normal, AUTH.Enhanced or AUTH.Strong:
 - initiate a connection between the internet connected toy and its communication partner;
 - attempt to capture data (user credentials, tokens, etc.) with the tool in place and actively intercept communication to impersonate the communication partner during:
 - generation and communication of authentication factor for the communication partner (if not pre-configured); and
 - authentication of the communication partner.
 - record if the impersonation as communication partner is successful.

Assessment verdict:

The verdict PASS shall be assigned if:

- the authentication mechanism does not accept the PitM as an authenticated entity.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- description of the performed test;
- all test records of the performed test.

E.2 Integrity protection strength

E.2.1 [INT-SSM] Integrity protecting persistent storage for integrity relevant data

E.2.1.1 General

Specific requirements on integrity protecting secure storage mechanisms for the INT-SSM strength level determined in clause [5.8.1](#).

E.2.1.2 [INT-SSM-E-Basic] INT.SSM.Basic integrity protecting secure storage mechanism

Where an integrity protecting secure storage mechanism is used to achieve INT.SSM.Basic, the integrity protecting secure storage mechanism shall use cryptographic protection measures to protect against targeted modification of stored data, using a confidential cryptographic key with a $L_{CP,eff}$ of minimal 112 bit.

NOTE: Protection against targeted modification of stored data can amongst others be achieved by appropriate storage encryption.

E.2.1.3 [INT-SSM-E-Normal] INT.SSM.Normal integrity protecting secure storage mechanism

Where an integrity protecting secure storage mechanism is used to achieve INT.SSM.Normal, the integrity protecting secure storage mechanism shall:

- use cryptographic protection measures to protect against targeted modification of stored data, using a confidential cryptographic key with a $L_{CP,eff}$ of minimal 112 bit; and
- only decrypt after an authorised user is authenticated.

NOTE: Protection against targeted modification of stored data can amongst others be achieved by appropriate storage encryption.

E.2.1.4 [INT-SSM-E-Enhanced] INT.SSM.Enhanced integrity protecting secure storage mechanism

Where an integrity protecting secure storage mechanism is used to achieve INT.SSM.Enhanced, the integrity protecting secure storage mechanism shall:

- use cryptographic protection measures to protect against targeted modification of stored data, using a confidential cryptographic key with a $L_{CP,eff}$ of minimal 125 bit and - only decrypt after an authorised user is authenticated and - the confidential cryptographic key is protected against unauthorised access by hardware measures.

NOTE: Protection against targeted modification of stored data can amongst others be achieved by appropriate storage encryption.

E.2.1.5 [INT-SSM-E-Strong] INT.SSM.Strong integrity protecting secure storage mechanism

Where an integrity protecting secure storage mechanism is used to achieve INT.SSM.Strong, the integrity protecting secure storage mechanism shall prevent the physical modification of data by hardware.

E.2.2 Assessment for integrity protecting secure storage mechanism strength

E.2.2.1 General

Specific assessments on integrity protecting secure storage mechanisms for the INT-SSM strength level determined in clause [5.8.1](#).

E.2.2.2 Assessment criteria for [INT-SSM-E-Basic]

Assessment reference:

[\[INT-SSM-E-Basic\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an integrity protecting secure storage mechanism used by the internet connected toy to fulfil [INT-SSM] clause [5.8.1](#) for authentication level INT.SSM.Basic.

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the integrity protecting secure storage mechanism used by the internet connected toy to achieve INT.SSM.Basic:
 - documentation of the confidential cryptographic keys used to protect against targeted modification of stored data.

The following test setups shall be prepared:

- a test setup to access the documented integrity protecting secure storage mechanism.

Assessment activities:

The following activities shall be performed:

- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect against targeted modification of stored data.

Assessment verdict:

The verdict PASS shall be assigned if:

- the integrity protecting secure storage mechanism used to achieve INT.SSM.Basic uses only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit to protect against targeted modification of stored data; and
- there is no indication, that the integrity protecting secure storage mechanism used to achieve INT.SSM.Basic differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.2.2.3 Assessment criteria for [INT-SSM-E-Normal]**Assessment reference:**

[\[INT-SSM-E-Normal\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an integrity protecting secure storage mechanism used by the internet connected toy to fulfil [INT-SSM] clause [5.8.1](#) for authentication level INT.SSM.Basic.

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the integrity protecting secure storage mechanism used by the internet connected toy to achieve INT.SSM.Basic:
 - documentation of the confidential cryptographic keys used to protect against targeted modification of stored data.

The following test setups shall be prepared:

- a test setup to access the documented integrity protecting secure storage mechanism

Assessment activities:

The following activities shall be performed:

- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect against targeted modification of stored data;
- verify whether stored integrity relevant data is not targeted modifiable until an authorised user is authenticated.

Assessment verdict:

The verdict PASS shall be assigned if:

- the integrity protecting secure storage mechanism used to achieve INT.SSM.Basic uses only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit to protect against targeted modification of stored data; and
- stored integrity relevant data is not targeted modifiable until an authorised user is authenticated; and
- there is no indication, that the integrity protecting secure storage mechanism used to achieve INT.SSM.Basic differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.2.2.4 Assessment criteria for [INT-SSM-E-Enhanced]

Assessment reference:

[\[INT-SSM-E-Enhanced\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an integrity protecting secure storage mechanism used by the internet connected toy to fulfil [INT-SSM] clause [5.8.1](#) for authentication level INT.SSM.Enhanced,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the integrity protecting secure storage mechanism used by the internet connected toy to achieve INT.SSM.Enhanced:
 - documentation of the confidential cryptographic keys used to protect against targeted modification of stored data.

The following test setups shall be prepared:

- a test setup to access the documented integrity protecting secure storage mechanism.

Assessment activities:

The following activities shall be performed:

- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect against targeted modification of stored data;
- verify whether stored integrity relevant data is not targeted modifiable until an authorised user is authenticated;

- verify whether confidential cryptographic keys used to protect against targeted modification of stored data is protected against unauthorised access by hardware measures.

Assessment verdict:

The verdict PASS shall be assigned if:

- the integrity protecting secure storage mechanism used to achieve INT.SSM.Enhanced uses only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 125 bit to protect against targeted modification of stored data; and
- stored integrity relevant data is not targeted modifiable until an authorised user is authenticated; and
- the confidential cryptographic keys used to protect against targeted modification of stored data is protected against unauthorised access by hardware measures; and
- there is no indication, that the integrity protecting secure storage mechanism used to achieve INT.SSM.Enhanced differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.2.2.5 Assessment criteria for [INT-SSM-E-Strong]

Assessment reference:

[\[INT-SSM-E-Strong\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an integrity protecting secure storage mechanism used by the internet connected toy to fulfil [INT-SSM] clause [5.8.1](#) for authentication level INT.SSM.Strong.

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the integrity protecting secure storage mechanism used by the internet connected toy to achieve INT.SSM.Strong:
 - documentation of the hardware measures used to protect against targeted modification of stored data.

The following test setups shall be prepared:

- a test setup to access the documented integrity protecting secure storage mechanism.

Assessment activities:

The following activities shall be performed:

- verify whether against targeted modification of stored integrity relevant data is protected by hardware measures.

Assessment verdict:

The verdict PASS shall be assigned if:

- against targeted modification of stored integrity relevant data is protected by hardware measures; and

- there is no indication, that the integrity protecting secure storage mechanism used to achieve INT.SSM.Strong differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.2.3 [INT-COM] Communication of integrity relevant data

E.2.3.1 General

Specific requirements on integrity protecting communication mechanisms for the INT-COM strength level determined in clause 5.8.2. Note that for CONF.COM.Normal, CONF.COM.Enhanced and CONF.COM.Strong, the requirements in clause E.2.3.5 and clause E.2.3.6 are also to be considered.

E.2.3.2 [INT-COM-E-Basic] INT.COM.Basic integrity protecting communication mechanism

Where an integrity protecting communication mechanism is used to achieve INT.COM.Basic, the integrity protecting communication mechanism shall use confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit to protect the integrity of communicated integrity relevant data.

NOTE: The values used for effective cryptographic security parameter bitlength are based on IETF RFC 8446 [i.10], IETF RFC 8613 [i.11], IETF RFC 9528 [i.12] and IETF RFC 9147 [i.13].

E.2.3.3 [INT-COM-E-Normal] INT.COM.Normal integrity protecting communication mechanism

Where an integrity protecting communication mechanism is used to achieve INT.COM.Basic, the integrity protecting communication mechanism shall use confidential cryptographic keys with:

- a $L_{CP,eff}$ of minimal 112 bit; or
- where maximal 1 GB of data of data can be communicated between rekeys due to bandwidth or power constraints, a $L_{CP,eff}$ of minimal 112 bit,

to protect the integrity of communicated integrity relevant data.

NOTE: The values used for effective cryptographic security parameter bitlength are based on IETF RFC 8446 [i.10], IETF RFC 8613 [i.11], IETF RFC 9528 [i.12] and IETF RFC 9147 [i.13].

E.2.3.4 [INT-COM-E-Enhanced] INT.COM.Enhanced integrity protecting communication mechanism

Where an integrity protecting communication mechanism is used to achieve INT.COM.Basic, the integrity protecting communication mechanism shall use confidential cryptographic keys with:

- a $L_{CP,eff}$ of minimal 125 bit; or
- where maximal 1 GB of data of data can be communicated between rekeys due to bandwidth or power constraints, a $L_{CP,eff}$ of minimal 112 bit,

to protect the integrity of communicated integrity relevant data.

NOTE: The values used for effective cryptographic security parameter bitlength are based on IETF RFC 8446 [i.10], IETF RFC 8613 [i.11], IETF RFC 9528 [i.12] and IETF RFC 9147 [i.13].

E.2.3.5 [INT-COM-E-EndAuth] INT.COM.Normal and INT.COM.Enhanced integrity protecting communication mechanism endpoint authentication

Where an integrity protecting communication mechanism is used to achieve INT.COM.Normal or INT.COM.Enhanced, the integrity protecting communication mechanism shall support the authentication of communication endpoints.

E.2.3.6 [INT-COM-E-Downgrade] INT.COM.Normal and INT.COM.Enhanced integrity protecting communication mechanism downgrade protection

Where an integrity protecting communication mechanism is used to achieve INT.COM.Normal or INT.COM.Enhanced, the integrity protecting communication mechanism shall support measures to prevent downgrade of the integrity protecting communication mechanisms protection measures below the protection strength level required in clause [5.8.2](#).

E.2.4 Assessment for integrity protecting communication mechanism strength

E.2.4.1 General

Specific assessments on integrity protecting communication mechanisms for the INT-COM strength level determined in clause [5.8.2](#).

E.2.4.2 Assessment criteria for [INT-COM-E-Basic]

Assessment reference:

[\[INT-COM-E-Basic\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an integrity protecting communication mechanism used by the internet connected toy to fulfil [INT-COM] clause [5.8.2](#) for authentication level INT.COM.Basic,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the integrity protecting communication mechanism used by the internet connected toy to achieve INT.COM.Basic:
 - documentation of the confidential cryptographic keys used to protect the integrity of communicated integrity relevant data.

The following test setups shall be prepared:

- a test setup to access the documented integrity protecting communication mechanism via a documented interface.

Assessment activities:

The following activities shall be performed:

- verify whether the integrity protecting communication mechanism can be accessed via the documented interfaces;

- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect the integrity of communicated integrity relevant data.

Assessment verdict:

The verdict PASS shall be assigned if:

- the integrity protecting communication mechanism used to achieve INT.COM.Basic uses only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit to protect the integrity of communicated integrity relevant data; and
- there is no indication, that the integrity protecting communication mechanism used to achieve INT.COM.Basic differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.2.4.3 Assessment criteria for [INT-COM-E-Normal]

Assessment reference:

[\[INT-COM-E-Normal\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an integrity protecting communication mechanism used by the internet connected toy to fulfil [INT-COM] clause [5.8.2](#) for authentication level INT.COM.Normal,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the integrity protecting communication mechanism used by the internet connected toy to achieve INT.COM.Normal:
 - documentation of the confidential cryptographic keys used to protect the integrity of communicated integrity relevant data;
 - where the integrity protecting communication mechanism is constrained by power or bandwidth:
 - the amount of data that can be communicated in a given time.

The following test setups shall be prepared:

- a test setup to access the documented integrity protecting communication mechanism via a documented interface.

Assessment activities:

The following activities shall be performed:

- verify whether the integrity protecting communication mechanism can be accessed via the documented interfaces;
- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect the integrity of communicated integrity relevant data:
 - if the $L_{CP,eff}$ is between 100 bit and 112 bit:

- determine the time after which the confidential cryptographic keys used to protect the integrity of communicated integrity relevant data are renewed;
- determine the amount of data that can be communicated during this time.

Assessment verdict:

The verdict PASS shall be assigned if:

- there is no indication, that the integrity protecting communication mechanism used to achieve INT.COM.Normal differs from the documentation;
- the integrity protecting communication mechanism used to achieve INT.COM.Normal uses only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit to protect the integrity of communicated integrity relevant data; or
- if amount of data can be communicated during the time between the renewal of confidential cryptographic keys used to protect the integrity of communicated integrity relevant data is maximal 1 GB of data, only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.2.4.4 Assessment criteria for [INT-COM-E-Enhanced]

Assessment reference:

[\[INT-COM-E-Enhanced\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an integrity protecting communication mechanism used by the internet connected toy to fulfil [INT-COM] clause [5.8.2](#) for authentication level INT.COM.Enhanced,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the integrity protecting communication mechanism used by the internet connected toy to achieve INT.COM.Enhanced:
 - documentation of the confidential cryptographic keys used to protect the integrity of communicated integrity relevant data;
 - where the integrity protecting communication mechanism is constrained by power or bandwidth:
 - the amount of data that can be communicated in a given time.

The following test setups shall be prepared:

- a test setup to access the documented integrity protecting communication mechanism via a documented interface.

Assessment activities:

The following activities shall be performed:

- verify whether the integrity protecting communication mechanism can be accessed via the documented interfaces;

- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect the integrity of communicated integrity relevant data:
 - if the $L_{CP,eff}$ is between 112 bit and 125 bit:
 - determine the time after which the confidential cryptographic keys used to protect the integrity of communicated integrity relevant data are renewed;
 - determine the amount of data that can be communicated during this time.

Assessment verdict:

The verdict PASS shall be assigned if:

- there is no indication, that the integrity protecting communication mechanism used to achieve INT.COM.Enhanced differs from the documentation;
- the integrity protecting communication mechanism used to achieve INT.COM.Enhanced uses only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 125 bit to protect the integrity of communicated integrity relevant data; or
- if amount of data can be communicated during the time between the renewal of confidential cryptographic keys used to protect the integrity of communicated integrity relevant data is maximal 1 GB of data, only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.2.4.5 Assessment criteria for [INT-COM-E-EndAuth]

Assessment reference:

[\[INT-COM-E-EndAuth\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an integrity protecting communication mechanism used by the internet connected toy to fulfil [INT-COM] clause [5.8.2](#) for authentication level INT.COM.Normal or INT.COM.Enhanced,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the integrity protecting communication mechanism used by the internet connected toy to achieve INT.COM.Normal or INT.COM.Enhanced:
 - documentation of the measures to verify the authenticity of communication endpoints and to authenticate the integrity protecting communication mechanism or the architectural component.

The following test setups shall be prepared:

- a test setup to access the documented integrity protecting communication mechanism via a documented interface.

Assessment activities:

The following activities shall be performed:

- verify whether the integrity protecting communication mechanism supports authentication of communication endpoints before sending integrity relevant data;
- verify whether the integrity protecting communication mechanism supports authentication of itself or its architectural component to communication endpoints before the communication of integrity relevant data.

Assessment verdict:

The verdict PASS shall be assigned if:

- the integrity protecting communication mechanism supports authentication of communication endpoints before sending integrity relevant data; and
- the integrity protecting communication mechanism supports authentication of itself or its architectural component to communication endpoints before the communication of integrity relevant data.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.2.4.6 Assessment criteria for [INT-COM-E-Downgrade]

Assessment reference:

[\[INT-COM-E-Downgrade\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an integrity protecting communication mechanism used by the internet connected toy to fulfil [INT-COM] clause [5.8.2](#) for authentication level INT.COM.Normal or INT.COM.Enhanced,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the integrity protecting communication mechanism used by the internet connected toy to achieve INT.COM.Normal or INT.COM.Enhanced:
 - documentation of the measures to prevent the downgrade of the integrity protecting communication mechanisms protection level by communication endpoints.

The following test setups shall be prepared:

- a test setup to access the documented integrity protecting communication mechanism via a documented interface;
- a test setup to alter parameters of communication protocols, determining e.g. used protocol versions or cipher suites.

Assessment activities:

The following activities shall be performed:

- verify whether the integrity protecting communication mechanism refuses to send integrity relevant data using communication protocol parameters that would result in a protection level below INT.COM.Normal or INT.COM.Enhanced respectively
- verify whether the integrity protecting communication mechanism refuses alteration of communication protocol parameters that would result in a protection level below INT.COM.Normal or INT.COM.Enhanced during the communication of integrity relevant data

Assessment verdict:

The verdict PASS shall be assigned if:

- the integrity protecting communication mechanism refuses to send integrity relevant data using communication protocol parameters that would result in a protection level below INT.COM.Normal or INT.COM.Enhanced respectively; and
- the integrity protecting communication mechanism refuses alteration of communication protocol parameters that would result in a protection level below INT.COM.Normal or INT.COM.Enhanced during the communication of integrity relevant data.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.2.5 [INT-SWPCK] Software package verification

E.2.5.1 General

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

E.2.5.2 [INT-SWPCK-E-Basic] INT.SW.VER.Basic software package verification mechanism

Where an software package verification mechanism is used to achieve INT.SW.VER.Basic, the software package verification mechanism shall:

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

E.2.5.3 [INT-SWPCK-E-Normal] INT.SW.VER.Normal software package verification mechanism

Where an software package verification mechanism is used to achieve INT.SW.VER.Normal, the software package verification mechanism shall ensure that a software package has been obtained from a trusted source over a secure communication channel that meets INT.COM.Enhanced.

E.2.5.4 [INT-SWPCK-E-Enhanced] INT.SW.VER.Enhanced software package verification mechanism

Where an software package verification mechanism is used to achieve INT.SW.VER.Enhanced, the software package verification mechanism shall verify the authenticity and integrity of a software package using cryptographic digital signature with a $L_{CP,eff}$ of minimal 125 bit.

E.2.6 Assessment for integrity protecting communication mechanism strength

E.2.6.1 General

Specific assessments on integrity protecting communication mechanisms for the INT-SWPCK strength level determined in clause [5.8.3](#).

E.2.6.2 Assessment criteria for [INT-SWPCK-E-Basic]

Assessment reference:

[\[INT-SWPCK-E-Basic\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an software package verification mechanism used by the internet connected toy to fulfil [INT-SWPCK] clause [5.8.3](#) for authentication level INT.SW.VER.Basic,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the software package verification mechanism used by the internet connected toy to achieve INT.SW.VER.Basic:
 - documentation of the measures to confirm, that the integrity and authenticity of a software package has been verified.

The following test setups shall be prepared:

- a test identity with permissions to perform a software update using the software package verification mechanism;
- a software package to perform a software update;
- a test setup to access the documented software package verification mechanism and perform a software update.

Assessment activities:

The following activities shall be performed:

- verify whether the confirmation of an authorised identity that the integrity and authenticity of a software package has been verified by the authorised identity is explicitly obtained by the software package verification mechanism used to achieve INT.SW.VER.Basic; or
- verify whether the confirmation of an authorised identity that the authenticity of a software package has been verified by the authorised identity is explicitly obtained by the software package verification mechanism used to achieve INT.SW.VER.Basic; and

- verify whether an authorised identity is provided with a hash or checksum to verify the integrity of a software package by the software package verification mechanism used to achieve INT.SW.VER.Basic.

Assessment verdict:

The verdict PASS shall be assigned if:

- there is no indication, that by the software package verification mechanism used to achieve INT.SW.VER.Basic differs from the documentation; and either
- the confirmation of an authorised identity that the integrity and authenticity of a software package has been verified by the authorised identity is explicitly obtained by the software package verification mechanism used to achieve INT.SW.VER.Basic; or
- the confirmation of an authorised identity that the authenticity of a software package has been verified by the authorised identity is explicitly obtained by the software package verification mechanism used to achieve INT.SW.VER.Basic; and
- an authorised identity is provided with a hash or checksum to verify the integrity of a software package by the software package verification mechanism used to achieve INT.SW.VER.Basic.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.2.6.3 Assessment criteria for [INT-SWPCK-E-Normal]

Assessment reference:

[\[INT-SWPCK-E-Normal\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an software package verification mechanism used by the internet connected toy to fulfil [INT-SWPCK] clause [5.8.3](#) for authentication level INT.SW.VER.Normal,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the software package verification mechanism used by the internet connected toy to achieve INT.SW.VER.Normal
 - documentation of the measures to ensure that a software package has been obtained from a trusted source over a secure communication channel:
 - list of trusted source of software packages; or
 - documentation on criteria what comprises a trusted source of software packages.

The following test setups shall be prepared:

- a test identity with permissions to perform a software update using the software package verification mechanism;
- a communication connection to a trusted source of software packages to perform a software update;
- a test setup to access the documented software package verification mechanism and perform a software update.

Assessment activities:

The following activities shall be performed:

- verify whether the software package verification mechanism ensures that a software package has been obtained from a trusted source over a secure communication channel;
- verify whether the secure communication channel over which the software package has been obtained fulfils clause [E.2.3.4](#), clause [E.2.3.5](#) and clause [E.2.3.6](#).

Assessment verdict:

The verdict PASS shall be assigned if:

- the software package verification mechanism ensures that a software package has been obtained from a trusted source over a secure communication channel; and
- the secure communication channel over which the software package has been obtained fulfils clause [E.2.3.4](#), clause [E.2.3.5](#) and clause [E.2.3.6](#); and
- there is no indication, that by the software package verification mechanism used to achieve INT.SW.VER.Normal differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.2.6.4 Assessment criteria for [INT-SWPCK-E-Enhanced]

Assessment reference:

[\[INT-SWPCK-E-Enhanced\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an software package verification mechanism used by the internet connected toy to fulfil [INT-SWPCK] clause [5.8.3](#) for authentication level INT.SW.VER.Enhanced,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the software package verification mechanism used by the internet connected toy to achieve INT.SW.VER.Enhanced:
 - documentation of the measures to verify the integrity and authenticity of a software package using cryptographic digital signatures:
 - documentation of the cryptographic digital signatures used to verify the integrity and authenticity of a software package.

The following test setups shall be prepared:

- a test identity with permissions to perform a software update using the software package verification mechanism;
- software packages to perform a software update;
- a test setup to access the documented software package verification mechanism and perform a software update.

Assessment activities:

The following activities shall be performed:

- verify whether the software package verification mechanism verifies the integrity and authenticity of a software package using cryptographic digital signatures;
- determine the $L_{CP,eff}$ of the cryptographic digital signatures used to verify the integrity and authenticity of a software package.

Assessment verdict:

The verdict PASS shall be assigned if:

- the software package verification mechanism verifies the integrity and authenticity of a software package using cryptographic digital signatures; and
- the cryptographic digital signatures used to verify the integrity and authenticity of a software package have a $L_{CP,eff}$ of minimal 125 bit; and
- there is no indication, that by the software package verification mechanism used to achieve INT.SW.VER.Enhanced differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.3 Confidentiality protection strength

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

E.3.1.1 General

Specific requirements on integrity protecting secure storage mechanisms for the CONF-SSM strength level determined in clause [5.7.1](#).

E.3.1.2 [CONF-SSM-E-Basic] CONF.SSM.Basic confidentiality protecting secure storage mechanism

Where an confidentiality protecting secure storage mechanism is used to achieve CONF.SSM.Basic, the confidentiality protecting secure storage mechanism shall use cryptographic protection measures to protect the confidentiality of its stored confidential data, using a confidential cryptographic key with a $L_{CP,eff}$ of minimal 112 bit.

NOTE: The values used for effective cryptographic security parameter bitlength are based on IETF RFC 8446 [i.10], IETF RFC 8613 [i.11], IETF RFC 9528 [i.12] and IETF RFC 9147 [i.13].

E.3.1.3 [CONF-SSM-E-Normal] CONF.SSM.Normal confidentiality protecting secure storage mechanism

Where an confidentiality protecting secure storage mechanism is used to achieve CONF.SSM.Normal, the confidentiality protecting secure storage mechanism shall:

- use cryptographic protection measures to protect the confidentiality of its stored confidential data, using a confidential cryptographic key with a $L_{CP,eff}$ of minimal 112 bit; and

- only decrypt after an authorised user is authenticated.

NOTE: The values used for effective cryptographic security parameter bitlength are based on IETF RFC 8446 [i.10], IETF RFC 8613 [i.11], IETF RFC 9528 [i.12] and IETF RFC 9147 [i.13].

E.3.1.4 [CONF-SSM-E-Enhanced] CONF.SSM.Enhanced confidentiality protecting secure storage mechanism

Where an confidentiality protecting secure storage mechanism is used to achieve CONF.SSM.Enhanced, the confidentiality protecting secure storage mechanism shall:

- use cryptographic protection measures to protect the confidentiality of its stored confidential data, using a confidential cryptographic key with a $L_{CP,eff}$ of minimal 125 bit and - only decrypt after an authorised user is authenticated and - the confidential cryptographic key is protected against unauthorised access by hardware measures.

NOTE: The values used for effective cryptographic security parameter bitlength are based on IETF RFC 8446 [i.10], IETF RFC 8613 [i.11], IETF RFC 9528 [i.12] and IETF RFC 9147 [i.13].

E.3.1.5 [CONF-SSM-E-Strong] CONF.SSM.Strong confidentiality protecting secure storage mechanism

Where an confidentiality protecting secure storage mechanism is used to achieve CONF.SSM.Strong, the confidentiality protecting secure storage mechanism shall prevent extraction of its stored confidential data by hardware measures.

E.3.2 Assessment for integrity protecting secure storage mechanism strength

E.3.2.1 General

Specific assessments on integrity protecting secure storage mechanisms for the CONF-SSM strength level determined in clause [5.7.1](#).

E.3.2.2 Assessment criteria for [CONF-SSM-E-Basic]

Assessment reference:

[\[CONF-SSM-E-Basic\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an confidentiality protecting secure storage mechanism used by the internet connected toy to fulfil [CONF-SSM] clause [5.7.1](#) for authentication level CONF.SSM.Normal,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the confidentiality protecting secure storage mechanism used by the internet connected toy to achieve CONF.SSM.Normal:
 - documentation of the confidential cryptographic keys used to protect the confidentiality of stored confidential data.

The following test setups shall be prepared:

- a test setup to access the documented confidentiality protecting secure storage mechanism.

Assessment activities:

The following activities shall be performed:

- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect the confidentiality of stored confidential data.

Assessment verdict:

The verdict PASS shall be assigned if:

- the confidentiality protecting secure storage mechanism used to achieve CONF.SSM.Normal uses only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit to protect the confidentiality of stored confidential data; and
- there is no indication, that the confidentiality protecting secure storage mechanism used to achieve CONF.SSM.Normal differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.3.2.3 Assessment criteria for [CONF-SSM-E-Normal]

Assessment reference:

[\[CONF-SSM-E-Normal\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an confidentiality protecting secure storage mechanism used by the internet connected toy to fulfil [CONF-SSM] clause [5.7.1](#) for authentication level CONF.SSM.Basic.

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the confidentiality protecting secure storage mechanism used by the internet connected toy to achieve CONF.SSM.Basic:
 - documentation of the confidential cryptographic keys used to protect the confidentiality of stored confidential data.

The following test setups shall be prepared:

- a test setup to access the documented confidentiality protecting secure storage mechanism.

Assessment activities:

The following activities shall be performed:

- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect the confidentiality of stored confidential data;
- verify whether stored confidential data is not readably in plain text until an authorised user is authenticated.

Assessment verdict:

The verdict PASS shall be assigned if:

- the confidentiality protecting secure storage mechanism used to achieve CONF.SSM.Basic uses only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit to protect the confidentiality of stored confidential data; and
- stored confidential data is not readably in plain text until an authorised user is authenticated; and
- there is no indication, that the confidentiality protecting secure storage mechanism used to achieve CONF.SSM.Basic differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.3.2.4 Assessment criteria for [CONF-SSM-E-Enhanced]

Assessment reference:

[\[CONF-SSM-E-Enhanced\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an confidentiality protecting secure storage mechanism used by the internet connected toy to fulfil [CONF-SSM] clause [5.7.1](#) for authentication level CONF.SSM.Enhanced,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the confidentiality protecting secure storage mechanism used by the internet connected toy to achieve CONF.SSM.Enhanced:
 - documentation of the confidential cryptographic keys used to protect the confidentiality of stored confidential data.

The following test setups shall be prepared:

- a test setup to access the documented confidentiality protecting secure storage mechanism.

Assessment activities:

The following activities shall be performed:

- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect the confidentiality of stored confidential data;
- verify whether stored confidential data is not readably in plain text until an authorised user is authenticated;
- verify whether confidential cryptographic keys used to protect the confidentiality of stored confidential data is protected against unauthorised access by hardware measures.

Assessment verdict:

The verdict PASS shall be assigned if:

- the confidentiality protecting secure storage mechanism used to achieve CONF.SSM.Enhanced uses only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 125 bit to protect the confidentiality of stored confidential data; and
- stored confidential data is not readably in plain text until an authorised user is authenticated; and
- the confidential cryptographic keys used to protect the confidentiality of stored confidential data is protected against unauthorised access by hardware measures; and
- there is no indication, that the confidentiality protecting secure storage mechanism used to achieve CONF.SSM.Enhanced differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.3.2.5 Assessment criteria for [CONF-SSM-E-Strong]

Assessment reference:

[\[CONF-SSM-E-Strong\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an confidentiality protecting secure storage mechanism used by the internet connected toy to fulfil [CONF-SSM] clause [5.7.1](#) for authentication level CONF.SSM.Strong,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the confidentiality protecting secure storage mechanism used by the internet connected toy to achieve CONF.SSM.Strong:
 - documentation of the hardware measures used to protect the confidentiality of stored confidential data.

The following test setups shall be prepared:

- a test setup to access the documented confidentiality protecting secure storage mechanism.

Assessment activities:

The following activities shall be performed:

- verify whether the confidentiality of stored confidential data is protected by hardware measures.

Assessment verdict:

The verdict PASS shall be assigned if:

- the confidentiality of stored confidential data is protected by hardware measures; and
- there is no indication, that the confidentiality protecting secure storage mechanism used to achieve CONF.SSM.Strong differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.3.3 [CONF-COM] Communication of confidential data

E.3.3.1 General

Specific requirements on confidentiality protecting communication mechanisms for the CONF-COM strength level determined in clause 5.7.2. Note that for CONF.COM.Normal, CONF.COM.Enhanced and CONF.COM.Strong, the requirements in clause E.3.3.5 and clause E.3.3.6 are also to be considered.

E.3.3.2 [CONF-COM-E-Basic] CONF.COM.Basic confidentiality protecting communication mechanism

Where an confidentiality protecting communication mechanism is used to achieve CONF.COM.Basic, the confidentiality protecting communication mechanism shall use confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit to protect the confidentiality of communicated confidential data.

NOTE: The values used for effective cryptographic security parameter bitlength are based on IETF RFC 8446 [i.10], IETF RFC 8613 [i.11], IETF RFC 9528 [i.12] and IETF RFC 9147 [i.13].

E.3.3.3 [CONF-COM-E-Normal] CONF.COM.Normal confidentiality protecting communication mechanism

Where an confidentiality protecting communication mechanism is used to achieve CONF.COM.Basic, the confidentiality protecting communication mechanism shall use confidential cryptographic keys with:

- a $L_{CP,eff}$ of minimal 112 bit, or
- where maximal 1 GB of data of data can be communicated between rekeys due to bandwidth or power constraints, a $L_{CP,eff}$ of minimal 112 bit,

to protect the confidentiality of communicated confidential data.

NOTE: The values used for effective cryptographic security parameter bitlength are based on IETF RFC 8446 [i.10], IETF RFC 8613 [i.11], IETF RFC 9528 [i.12] and IETF RFC 9147 [i.13].

E.3.3.4 [CONF-COM-E-Enhanced] CONF.COM.Enhanced confidentiality protecting communication mechanism

Where an confidentiality protecting communication mechanism is used to achieve CONF.COM.Basic, the confidentiality protecting communication mechanism shall use confidential cryptographic keys with:

- a $L_{CP,eff}$ of minimal 125 bit; or
- where maximal 1 GB of data of data can be communicated between rekeys due to bandwidth or power constraints, a $L_{CP,eff}$ of minimal 112 bit,

to protect the confidentiality of communicated confidential data.

NOTE: The values used for effective cryptographic security parameter bitlength are based on IETF RFC 8446 [i.10], IETF RFC 8613 [i.11], IETF RFC 9528 [i.12] and IETF RFC 9147 [i.13].

E.3.3.5 [CONF-COM-E-EndAuth] CONF.COM.Normal and CONF.COM.Enhanced confidentiality protecting communication mechanism endpoint authentication

Where an confidentiality protecting communication mechanism is used to achieve CONF.COM.Normal or CONF.COM.Enhanced, the confidentiality protecting communication mechanism shall support the authentication of communication endpoints.

E.3.3.6 [CONF-COM-E-Downgrade] CONF.COM.Normal and CONF.COM.Enhanced confidentiality protecting communication mechanism downgrade protection

Where an confidentiality protecting communication mechanism is used to achieve CONF.COM.Normal or CONF.COM.Enhanced, the confidentiality protecting communication mechanism shall support measures to prevent downgrade of the confidentiality protecting communication mechanisms protection measures below the protection strength level required in clause [5.8.2](#).

E.3.4 Assessment for confidentiality protecting communication mechanism strength

E.3.4.1 General

Specific assessments on confidentiality protecting communication mechanisms for the CONF-COM strength level determined in clause [5.7.2](#).

E.3.4.2 Assessment criteria for [CONF-COM-E-Basic]

Assessment reference:

[\[CONF-COM-E-Basic\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an confidentiality protecting communication mechanism used by the internet connected toy to fulfil [CONF-COM] clause [5.7.2](#) for authentication level CONF.COM.Basic,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the confidentiality protecting communication mechanism used by the internet connected toy to achieve CONF.COM.Basic:
 - documentation of the confidential cryptographic keys used to protect the confidentiality of communicated confidential data.

The following test setups shall be prepared:

- a test setup to access the documented confidentiality protecting communication mechanism via a documented interface.

Assessment activities:

The following activities shall be performed:

- verify whether the confidentiality protecting communication mechanism can be accessed via the documented interfaces;
- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect the confidentiality of communicated confidential data.

Assessment verdict:

The verdict PASS shall be assigned if:

- the confidentiality protecting communication mechanism used to achieve CONF.COM.Basic uses only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit to protect the confidentiality of communicated confidential data; and
- there is no indication, that the confidentiality protecting communication mechanism used to achieve CONF.COM.Basic differs from the documentation.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.3.4.3 Assessment criteria for [CONF-COM-E-Normal]**Assessment reference:**

[\[CONF-COM-E-Normal\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an confidentiality protecting communication mechanism used by the internet connected toy to fulfil [CONF-COM] clause [5.7.2](#) for authentication level CONF.COM.Normal,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the confidentiality protecting communication mechanism used by the internet connected toy to achieve CONF.COM.Normal:
 - documentation of the confidential cryptographic keys used to protect the confidentiality of communicated confidential data;
 - where the confidentiality protecting communication mechanism is constrained by power or bandwidth:
 - the amount of data that can be communicated in a given time.

The following test setups shall be prepared:

- a test setup to access the documented confidentiality protecting communication mechanism via a documented interface.

Assessment activities:

The following activities shall be performed:

- verify whether the confidentiality protecting communication mechanism can be accessed via the documented interfaces;
- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect the confidentiality of communicated confidential data:
 - if the $L_{CP,eff}$ is between 100 bit and 112 bit:
 - determine the time after which the confidential cryptographic keys used to protect the confidentiality of communicated confidential data are renewed;
 - determine the amount of data that can be communicated during this time.

Assessment verdict:

The verdict PASS shall be assigned if:

- there is no indication, that the confidentiality protecting communication mechanism used to achieve CONF.COM.Normal differs from the documentation; and
- the confidentiality protecting communication mechanism used to achieve CONF.COM.Normal uses only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit to protect the confidentiality of communicated confidential data; or
- if amount of data can be communicated during the time between the renewal of confidential cryptographic keys used to protect the confidentiality of communicated confidential data is maximal 1 GB of data, only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.3.4.4 Assessment criteria for [CONF-COM-E-Enhanced]**Assessment reference:**

[\[CONF-COM-E-Enhanced\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an confidentiality protecting communication mechanism used by the internet connected toy to fulfil [CONF-COM] clause [5.7.2](#) for authentication level CONF.COM.Enhanced,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the confidentiality protecting communication mechanism used by the internet connected toy to achieve CONF.COM.Enhanced:
 - documentation of the confidential cryptographic keys used to protect the confidentiality of communicated confidential data;
 - where the confidentiality protecting communication mechanism is constrained by power or bandwidth:
 - the amount of data that can be communicated in a given time.

The following test setups shall be prepared:

- a test setup to access the documented confidentiality protecting communication mechanism via a documented interface.

Assessment activities:

The following activities shall be performed:

- verify whether the confidentiality protecting communication mechanism can be accessed via the documented interfaces;
- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect the confidentiality of communicated confidential data:
 - if the $L_{CP,eff}$ is between 112 bit and 125 bit:
 - determine the time after which the confidential cryptographic keys used to protect the confidentiality of communicated confidential data are renewed;
 - determine the amount of data that can be communicated during this time.

Assessment verdict:

The verdict PASS shall be assigned if:

- there is no indication, that the confidentiality protecting communication mechanism used to achieve CONF.COM.Enhanced differs from the documentation; and
- the confidentiality protecting communication mechanism used to achieve CONF.COM.Enhanced uses only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 125 bit to protect the confidentiality of communicated confidential data; or
- if amount of data can be communicated during the time between the renewal of confidential cryptographic keys used to protect the confidentiality of communicated confidential data is maximal 1 GB of data, only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.3.4.5 Assessment criteria for [CONF-COM-E-EndAuth]

Assessment reference:

[\[CONF-COM-E-EndAuth\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an confidentiality protecting communication mechanism used by the internet connected toy to fulfil [CONF-COM] clause [5.7.2](#) for authentication level CONF.COM.Normal or CONF.COM.Enhanced,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the confidentiality protecting communication mechanism used by the internet connected toy to achieve CONF.COM.Normal or CONF.COM.Enhanced:
 - documentation of the measures to verify the authenticity of communication endpoints and to authenticate the confidentiality protecting communication mechanism or the architectural component.

The following test setups shall be prepared:

- a test setup to access the documented confidentiality protecting communication mechanism via a documented interface.

Assessment activities:

The following activities shall be performed:

- verify whether the confidentiality protecting communication mechanism supports authentication of communication endpoints before sending confidential data;
- verify whether the confidentiality protecting communication mechanism supports authentication of itself or its architectural component to communication endpoints before the communication of confidential data.

Assessment verdict:

The verdict PASS shall be assigned if:

- the confidentiality protecting communication mechanism supports authentication of communication endpoints before sending confidential data; and
- the confidentiality protecting communication mechanism supports authentication of itself or its architectural component to communication endpoints before the communication of confidential data.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

E.3.4.6 Assessment criteria for [CONF-COM-E-Downgrade]

Assessment reference:

[\[CONF-COM-E-Downgrade\]](#)

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an confidentiality protecting communication mechanism used by the internet connected toy to fulfil [CONF-COM] clause [5.7.2](#) for authentication level CONF.COM.Normal or CONF.COM.Enhanced,

based on the default configuration required by clause [5.4](#).

Assessment preparation:

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

- for the confidentiality protecting communication mechanism used by the internet connected toy to achieve CONF.COM.Normal or CONF.COM.Enhanced:
 - documentation of the measures to prevent the downgrade of the confidentiality protecting communication mechanisms protection level by communication endpoints.

The following test setups shall be prepared:

- a test setup to access the documented confidentiality protecting communication mechanism via a documented interface;
- a test setup to alter parameters of communication protocols, determining e.g. used protocol versions or cipher suites.

Assessment activities:

The following activities shall be performed:

- verify whether the confidentiality protecting communication mechanism refuses to send confidential data using communication protocol parameters that would result in a protection level below CONF.COM.Normal or CONF.COM.Enhanced respectively;
- verify whether the confidentiality protecting communication mechanism refuses alteration of communication protocol parameters that would result in a protection level below CONF.COM.Normal or CONF.COM.Enhanced during the communication of confidential data.

Assessment verdict:

The verdict PASS shall be assigned if:

- the confidentiality protecting communication mechanism refuses to send confidential data using communication protocol parameters that would result in a protection level below CONF.COM.Normal or CONF.COM.Enhanced respectively; and
- the confidentiality protecting communication mechanism refuses alteration of communication protocol parameters that would result in a protection level below CONF.COM.Normal or CONF.COM.Enhanced during the communication of confidential data.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- all test records of the performed test.

Annex F (informative):

Guidance for the application of the present document

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

- to develop products that are compliant to; or
- to analyse the compliance of a product to the present document.
- Step 1 - check if the product is in scope of the present document provided in clause [1](#) by:
 - verifying that the product meets the "technical description" of the "category of product" number "18." by Commission Implementing Regulation (EU) 2025/2392 [i.2]; and
 - identifying the product context by:
 - identifying the product's architectural components; and
 - identifying all data processed by the product (data assets); and
 - identifying all functions provided by the product (function assets); and
 - identifying the architectural components' operational environments; and
 - identifying the architectural components' interfaces and communication types; and
 - verifying that the product is covered within the product context described in clause [4](#) by:
 - verifying that the architectural components of the product are covered within the product architecture described in clause [4.2](#); and
 - verifying that the data processed by the product and the functions provided by the product are covered within clause [4.1](#); and
 - verifying that the architectural components' operational environments are covered within clause [4.3](#); and
 - verifying that the architectural components' interfaces and communication types are covered within clause [4.3.4](#).

NOTE 1: The identification of the items mentioned above can be reused for assessing the compliance of the product with the requirements in clause [5](#).

NOTE 2: If a product meets the "technical description" of the "category of product" number "18." by Regulation (EU) 2025/2392 [i.2] but is not covered within the product context described in clause [4](#), it is assumed that the product is not or not completely covered by the present document. Such cases should be notified to ETSI at the following e-mail address: cybersupport@etsi.org to consider those products in potential revisions of the present document

- Step 2 - identify information to determine risk factors by:
 - identifying for each function provided by the product:
 - its impact classes according to clause [D.2](#); and
 - the architectural components that perform the function; and
 - the communication types and the interfaces that can receive corresponding function trigger input; and
 - identifying for each data processed by the product:
 - its impact classes according to clause [D.1](#)
 - the architectural components that persistently store the data; and

- the architectural components that can communicate the data; and
- the communication types and the interfaces over which the data is communicated.
- Step 3 - identify concrete requirements for and specific security measures/mitigations of the product that satisfy those requirements by:
 - for each requirement in clause 5:
 - identifying the requirements applicability by evaluating the requirement's potential preconditions and exceptions based on the product's properties; and
 - (for requirements that include assignment tables) identifying the required protection mechanisms' strengths (specified in annex E) by evaluating the requirement's assignment table based on the product's properties determining the attack surface and impact parameters; and
 - identifying the specific security measures/mitigations that satisfy the requirement.

NOTE 3: An assignment table can yield multiple mechanisms' strengths from different circumstances, which all have to be satisfied.

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

- Step 4 - assess the compliance of the product with the requirements in clause 5 by:
 - for each requirement in clause 5, performing the corresponding assessment for compliance described in clause 6 (the functional sufficiency assessments for different protection measures strengths are specified in annex E) by:
 - preparing the assessment for the product; and
 - performing the assessment activities for the product; and
 - assigning an assessment verdict for the product; and
 - generating the assessment evidences for the assessment.

Figure E.1 provides a graphical representation of the guidance for the application of the present document.

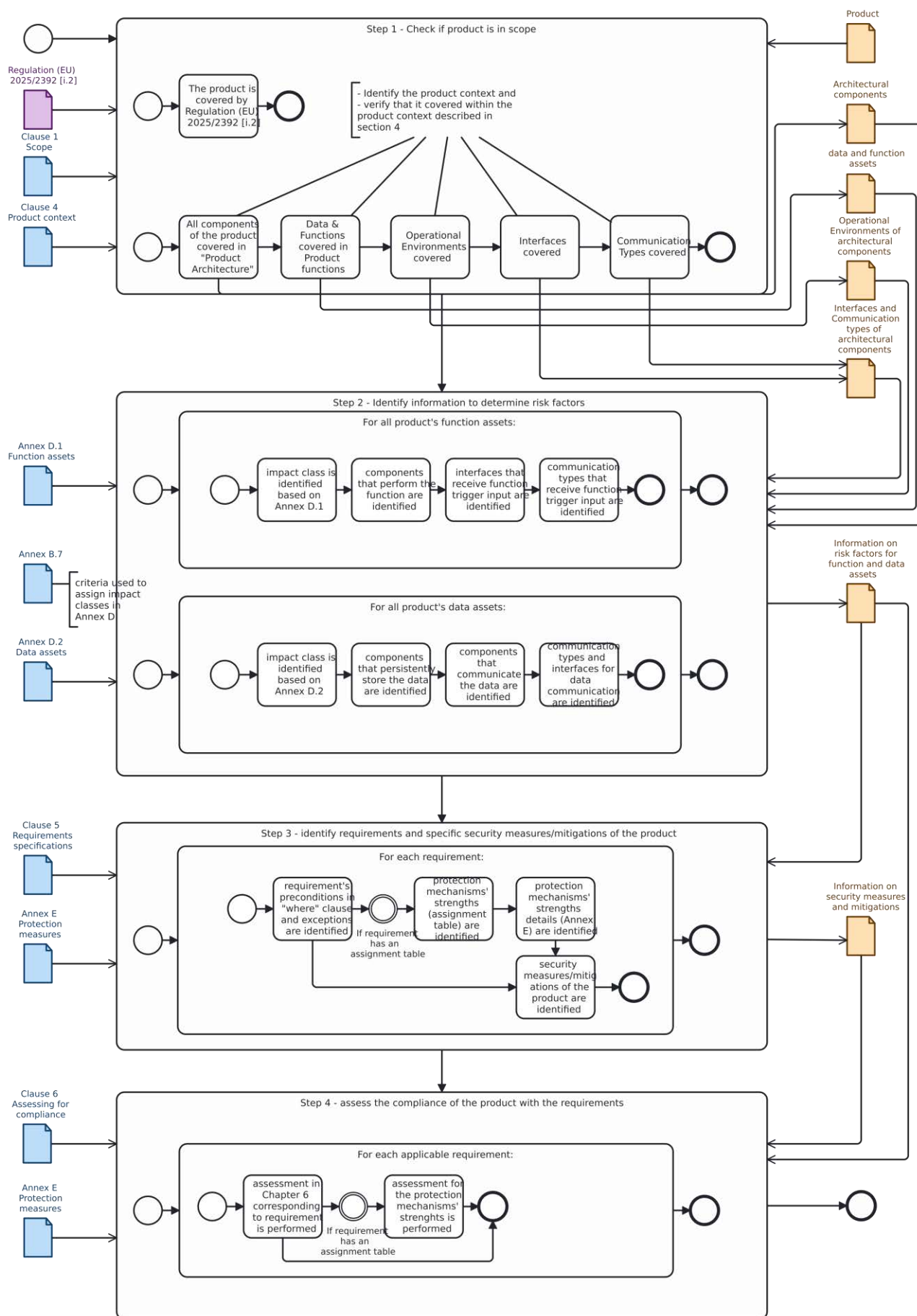


Figure F.1: Graphical representation on guidance for the application of the present document

Annexes G to J:
Void

Annex K (normative): Generic cryptographic requirements and assessment

K.1 Cryptography

K.1.1 [CRY-SOTA] Requirement

The internet connected toy's default configuration shall only use cryptographic mechanisms that meet at least one of the following criteria

- 1) ACM-listed: the cryptographic mechanism is listed in Agreed Cryptographic Mechanisms [1]; or
- 2) ACM-extended: the cryptographic mechanism is not listed Agreed Cryptographic Mechanisms [1] and meets at least one of the following conditions:
 - a) the cryptographic mechanism is listed in clause K.3.2 as an ACM-extended cryptographic mechanism for the specific internet connected toy function(s);
 - b) where the cryptographic mechanism is not listed in clause K.3.2, the cryptographic mechanism meets all the following criteria:
 - i) the cryptographic mechanism, or where applicable the ACM-listed cryptographic mechanism on which it is based, is not deprecated per Agreed Cryptographic Mechanisms [1];
 - ii) the cryptographic mechanism has been specified, developed or maintained through a transparent process by a recognised European, international or sector-specific standards development organisation, or by an industry specification organisation accountable for the relevant specification; or the cryptographic mechanism is listed as suitable in a publicly available cryptographic catalogue maintained by a recognised national or governmental cybersecurity authority, where the catalogue is maintained under a documented revision and retirement process;
 - iii) the cryptographic mechanism is described in a valid, publicly available and uniquely referenceable specification;
 - iv) the cryptographic properties of the cryptographic mechanism are known; v)no known weakness affects the cryptographic mechanism in a way that affects its cryptographic properties;
 - v) no known weakness affects the cryptographic mechanism in a way that affects its cryptographic properties;
 - vi) the cryptographic mechanism is required for a specific set of internet connected toy functions.
- 3) Interoperability-based: the cryptographic mechanism is listed in clause K.4.2 as an interoperability-based cryptographic mechanism for specific internet connected toy function(s) and external specification(s) or external requirement(s).

EXAMPLE: Examples of product functions include secure communication based on TLS 1.3; authenticated encryption of communicated data based on AES-GCM; storage confidentiality based on AES-XTS; firmware signature verification based on Ed25519; and key derivation based on HKDF.

NOTE 1: The reference to the internet connected toy's default configuration is intended to define a clear and assessable baseline, corresponding to the configuration in which the internet connected toy is placed on the market. The internet connected toy can provide several configurations that fulfil the requirement.

NOTE 2: For internet connected toys supplied as hardware platforms or components to be configured by an integrator, references in this annex to the internet connected toy's default configuration refer to the configuration specified for the intended operational use of the internet connected toy after integration, including the relevant integration assumptions and configuration constraints.

NOTE 3: The applicable Agreed Cryptographic Mechanisms (ACM) [1] catalogue version is identified in the normative references of the present document. The lifecycle treatment of mechanisms affected by Agreed Cryptographic Mechanisms [1] deprecation dates, expiry dates, migration conditions or usage limitations is addressed in clause K.2.

NOTE 4: In this clause, an external specification or external requirement means a specification or requirement that is imposed on the internet connected toy, and which requires the use of a specific cryptographic mechanism for the internet connected toy to interoperate with an identified system, platform or operational context. An external requirement can be a regulatory requirement, operational constraint, technical interoperability constraint, or platform compatibility requirement.

NOTE 5: Inclusion of a cryptographic mechanism under the interoperability-based criterion does not classify that mechanism as state-of-the-art cryptography.

K.1.2 Assessment criteria

K.1.2.1 Assessment criteria for [CRY-SOTA] concerning ACM-listed cryptographic mechanisms

Assessment reference:

[\[CRY-SOTA\]](#) concerning ACM-listed cryptographic mechanisms

Assessment objective:

The purpose of this assessment case is to verify that cryptographic mechanisms claimed to comply with clause K.1.1 item 1) and used in the product's default configuration are listed in Agreed Cryptographic Mechanisms [1].

Assessment preparation:

- Preconditions for the assessment: The product's default configuration shall be used for the assessment.
- The documentation shall provide a list of cryptographic mechanisms used in the product's default configuration and claimed under clause K.1.1 item 1), including the related product function, relevant parameters where applicable, and the relevant ACM entry.

Assessment activities:

The assessment shall include verification that:

- each cryptographic mechanism claimed under clause K.1.1 item 1) is identified by reference to a relevant ACM entry;
- the ACM entry corresponds to the cryptographic mechanism used in the product's default configuration, including relevant parameters where applicable;
- where the ACM entry includes lifecycle information, such as expiry date, deprecation date, migration condition or usage limitation, this information is reflected in the documentation.

Assessment verdict:

- The verdict PASS shall be assigned if the required evidence has been provided, is complete, is applicable to the assessed configuration, and demonstrates compliance with clause K.1.1 item 1).
- The verdict FAIL shall be assigned otherwise.

Assessment evidence:

The assessment evidence shall include, as applicable:

- description of the product's default configuration;
- list of cryptographic mechanisms claimed under clause K.1.1 item 1);

- references to the relevant ACM entries;
- relevant parameters, profiles, cipher suites or configuration constraints, where applicable;
- relevant lifecycle information from the ACM catalogue, where applicable.

K.1.2.2 Assessment criteria for [CRY-SOTA] concerning ACM-extended cryptographic mechanisms

Assessment reference:

[\[CRY-SOTA\]](#) concerning ACM-extended cryptographic mechanisms

Assessment objective:

The purpose of this assessment case is to verify that cryptographic mechanisms claimed to comply with clause K.1.1 item 2) and used in the product's default configuration are either listed as ACM-extended cryptographic mechanisms in clause K.3.2 or fulfil the criteria specified in clause K.1.1 item 2.b, and are used for the claimed product function(s).

Assessment preparation:

- Preconditions for the assessment: The product's default configuration shall be used for the assessment.
- The documentation shall provide a list of cryptographic mechanisms used in the product's default configuration and claimed under clause K.1.1 item 2), including the related product function, use case where applicable, relevant parameters where applicable, and at least one of the following:
 - the relevant entry in clause K.3.2; or
 - evidence that the cryptographic mechanism fulfils all applicable criteria in clause K.1.1 item 2.b.

Assessment activities:

The assessment shall include verification that:

- each cryptographic mechanism claimed under clause K.1.1 item 2) is either listed in clause K.3.2 as an ACM-extended cryptographic mechanism or supported by evidence demonstrating fulfilment of the applicable criteria in clause K.1.1 item 2.b;
- the cryptographic mechanism used by the product corresponds to the mechanism listed in clause K.3.2 or described in the evidence provided under clause K.1.1 item 2.b;
- the product function using the cryptographic mechanism, and the use case where applicable, correspond to the related product function and use case specified in clause K.3.2 or justified under clause K.1.1 item 2.b;
- the relevant characteristics, parameters, profiles, cipher suites or configuration constraints of the cryptographic mechanism correspond to those specified in clause K.3.2 or justified under clause K.1.1 item 2.b, where applicable;
- where clause K.3.2 or the justification under clause K.1.1 item 2.b defines conditions or limitations for the use of the cryptographic mechanism, these conditions or limitations are reflected in the product's default configuration;
- where technically feasible, the cryptographic mechanism, parameters and configuration identified in the documentation correspond to the assessed product configuration.

Assessment verdict:

- The verdict PASS shall be assigned if the required evidence has been provided, is complete, is applicable to the assessed configuration, and demonstrates compliance with clause K.1.1 item 2).
- The verdict FAIL shall be assigned otherwise.

Assessment evidence:

The assessment evidence shall include, as applicable:

- description of the product's default configuration;
- list of cryptographic mechanisms claimed under clause K.1.1 item 2);
- reference to the relevant entry in clause K.3.2, where the mechanism is listed in clause K.3.2;
- evidence that the cryptographic mechanism fulfils the criteria in clause K.1.1 item 2.b, where compliance with clause K.1.1 item 2 is claimed on the basis of those criteria;
- identification of the related product function using the cryptographic mechanism and the use case where applicable;
- relevant characteristics, parameters, profiles, cipher suites or configuration constraints, where applicable;
- evidence that the cryptographic mechanism is used in accordance with the conditions or limitations specified in clause K.3.2 or in the justification under clause K.1.1 item 2.b, where applicable.

K.1.2.3 Assessment criteria for [CRY-SOTA] concerning interoperability-based cryptographic mechanisms

Assessment reference:

[\[CRY-SOTA\]](#) concerning interoperability-based cryptographic mechanisms

Assessment objective:

The purpose of this assessment case is to verify that cryptographic mechanisms claimed to comply with clause K.1.1 item 3) and used in the product's default configuration are listed as interoperability-based cryptographic mechanisms in clause K.4.2 and are used in accordance with the characteristics, product functions, use cases where applicable, external specifications or external requirements, and conditions specified in clause K.4.2.

Assessment preparation:

- Preconditions for the assessment: The product's default configuration shall be used for the assessment.
- The documentation shall provide a list of cryptographic mechanisms used in the product's default configuration and claimed under clause K.1.1 item 3), including the related product function, use case where applicable, relevant parameters where applicable, the external specification or external requirement requiring its use, and the relevant entry in clause K.4.2.

Assessment activities:

The assessment shall include verification that:

- each cryptographic mechanism claimed under clause K.1.1 item 3) is listed in clause K.4.2 as an interoperability-based cryptographic mechanism;
- the cryptographic mechanism used by the product corresponds to the cryptographic mechanism listed in clause K.4.2;
- the product function using the cryptographic mechanism, and the use case where applicable, correspond to the related product function and use case specified in clause K.4.2;
- the external specification or external requirement requiring the use of the cryptographic mechanism corresponds to the external specification or external requirement specified in clause K.4.2;
- the relevant characteristics, parameters, profiles, cipher suites or configuration constraints of the cryptographic mechanism correspond to those specified in clause K.4.2, where applicable;
- the conditions or limitations specified in clause K.4.2 for the use of the cryptographic mechanism are reflected in the product's default configuration;

- where technically feasible, the cryptographic mechanism, parameters and configuration identified in the documentation correspond to the assessed product configuration.

Assessment verdict:

- The verdict PASS shall be assigned if the required evidence has been provided, is complete, is applicable to the assessed configuration, and demonstrates compliance with clause K.1.1 item 3).
- The verdict FAIL shall be assigned otherwise.

NOTE 1: The assessment of the external specification or external requirement itself is outside the scope of this assessment case. The assessment verifies that the external specification or external requirement is identified in clause K.4.2 and that the cryptographic mechanism is used by the product for the related product function.

NOTE 2: Documentation review is a minimum assessment activity under the present annex. Functional and/or resistance testing activities can be added by vertical standards where relevant for the product category, product function or cryptographic mechanism.

Assessment evidence:

The assessment evidence shall include, as applicable:

- description of the product's default configuration;
- list of cryptographic mechanisms claimed under clause K.1.1 item 3);
- reference to the relevant entry in clause K.4.2;
- identification of the related product function using the cryptographic mechanism and the use case where applicable;
- identification of the external specification or external requirement requiring use of the cryptographic mechanism;
- relevant characteristics, parameters, profiles, cipher suites or configuration constraints, where applicable;
- evidence that the cryptographic mechanism is used in accordance with the conditions or limitations specified in clause K.4.2.

K.2 Crypto agility

K.2.1 [CRY-AGIL] Requirement

Where the internet connected toy's default configuration uses a cryptographic mechanism for which the ACM catalogue Agreed Cryptographic Mechanisms [1], or the present document, specifies a deprecation date, expiry date, migration condition or usage limitation falling within the intended lifetime of the internet connected toy, the internet connected toy shall provide means for addressing the affected cryptographic mechanism by one or more of the following:

- updating the cryptographic mechanism;
- using another cryptographic mechanism that complies with clause K.1.1 and is not subject to the relevant deprecation date, expiry date, migration condition or usage limitation;
- disabling the use of the affected cryptographic mechanism; or
- limiting the use of the affected product functions accordingly.

EXAMPLE: Where a security mechanism uses a hybrid cryptographic construction, for example a hybrid key-encapsulation mechanism combining a classical and a post-quantum primitive, the lifecycle status of each constituent primitive is relevant to the lifecycle status of the construction. Hybridisation can be used as part of a planned migration strategy where permitted by the ACM catalogue or by the present document. However, hybridisation does not, by itself, extend the recommended usage lifetime of a constituent primitive that has been deprecated.

NOTE 1: Where a hybrid cryptographic construction includes multiple cryptographic primitives, the lifecycle status of each constituent primitive is relevant to the lifecycle status of the construction. Hybridisation is not assumed to mitigate the deprecation of a constituent primitive unless the ACM catalogue or the present document classifies the hybrid construction as suitable for the corresponding product function.

NOTE 2: Crypto agility supports maintaining appropriate cryptographic protection within the intended lifetime of the product, in addition to the capability of updating cryptographic mechanisms on the product in accordance with secure update and secure communication mechanisms.

NOTE 3: Deprecation information from sources other than the ACM catalogue or the present document can be considered as input to vulnerability management or security risk assessment but does not by itself trigger the requirement in clause K.2.1.

NOTE 4: Where the product provides cryptographic capabilities for use by other products, components or layers, the mechanism required by clause K.2.1 can consist of update, configuration, disabling, deprecation or limitation capabilities usable by the integrating product, system operator or user, where applicable.

NOTE 5: The applicability condition of this requirement can express exceptions based on product characteristics, e.g. cryptographic implementation based on immutable hardware co-processor(s) or hardware-based root of trust, or long-lived silicon used in a long-lived non-updateable environment.

K.2.2 Assessment criteria for [CRY-AGIL]

Assessment reference:

[\[CRY-AGIL\]](#)

Assessment objective:

The purpose of this assessment case is to verify whether, where the product's default configuration uses a cryptographic mechanism for which the ACM catalogue, or the present document, specifies a deprecation date, expiry date, migration condition or usage limitation falling within the intended lifetime of the product, the product provides means to address the affected cryptographic mechanism in accordance with clause K.2.1.

Assessment preparation:

- Preconditions for the assessment: The product's default configuration shall be used for the assessment.
- The documentation shall identify:
 - the intended lifetime of the product;
 - the cryptographic mechanisms used in the product's default configuration;
 - the related product function(s) for each cryptographic mechanism;
 - the lifecycle information applicable to each cryptographic mechanism, where specified by the ACM catalogue or the present document, including any deprecation date, expiry date, migration condition or usage limitation.

Assessment activities:

The assessment shall include verification that:

- for each cryptographic mechanism used in the product's default configuration, the lifecycle information specified by the ACM catalogue or the present document has been identified, where such information is specified;

- where the ACM catalogue or the present document specifies a deprecation date, expiry date, migration condition or usage limitation for a cryptographic mechanism, this information is reflected in the documentation;
- where a deprecation date, expiry date, migration condition or usage limitation falls within the intended lifetime of the product, the product provides an applicable mechanism for updating the cryptographic mechanism, using another cryptographic mechanism that complies with clause K.1.1 and is not subject to the relevant deprecation date, expiry date, migration condition or usage limitation, disabling the use of the affected cryptographic mechanism, or limiting the use of the affected product functions accordingly;
- where another cryptographic mechanism is used, that cryptographic mechanism complies with clause K.1.1 and is not subject to the relevant deprecation date, expiry date, migration condition or usage limitation.

Assessment verdict:

- The verdict PASS shall be assigned if the required evidence has been provided, is complete, is applicable to the assessed configuration, and demonstrates compliance with clause K.2.1.
- The verdict FAIL shall be assigned otherwise.

Assessment evidence:

The assessment evidence shall include, as applicable:

- documentation of the intended lifetime of the product;
- list of cryptographic mechanisms used in the product's default configuration;
- identification of the related product function(s) for each cryptographic mechanism;
- references to the ACM catalogue entry or to the provision of the present document used to determine lifecycle information, where applicable;
- identification of any deprecation date, expiry date, migration condition or usage limitation falling within the intended lifetime of the product;
- description of the means provided by the product, such as update of the cryptographic mechanism, use of another cryptographic mechanism that complies with clause K.1.1 and is not subject to the relevant lifecycle constraint, disabling the use of the affected cryptographic mechanism, or limitation of the use of the affected product functions.

K.3 ACM-extended cryptographic mechanisms

K.3.1 [CRY-ACM-EXT] Requirement

Where the internet connected toy's default configuration uses ACM-extended cryptographic mechanisms, these mechanisms shall comply with the ACM-extended criterion in clause K.1.1 item 2.

K.3.2 List of ACM-extended cryptographic mechanisms

Table K.1: ACM-extended cryptographic mechanisms

ACM-extended cryptographic mechanism	Type of cryptographic mechanism	Characteristics / parameters	Related product function(s) / use case(s), where applicable	Cryptographic properties	Specification / reference	Conditions or limitations, where applicable
<mechanism name>	<Algorithm / Primitive / Scheme / Protocol / Protocol profile / Cipher suite / Mode / Construction / Parameter set / Other>	<key length, mode, profile, cipher suite, parameter set, version, etc.>	<product function, interface, protocol context, operational context, etc.>	<confidentiality, integrity, authentication, key establishment, etc.>	<publicly available and uniquely referenceable specification>	<constraints, permitted use, excluded use, configuration limitation, lifecycle limitation, etc.>

K.3.3 Assessment

Compliance with the ACM-extended criterion in clause K.1.1 item 2 is assessed in clause K.1.2.2.

K.4 Interoperability-based cryptographic mechanisms

K.4.1 [CRY-INTOP] Requirement

Where the internet connected toy's default configuration uses interoperability-based cryptographic mechanisms, these mechanisms shall be selected from the interoperability-based cryptographic mechanisms listed in clause K.4.2 for the specified product functions and external specifications or external requirements and shall be used in accordance with the conditions or limitations specified in clause K.4.2.

K.4.2 List of interoperability-based cryptographic mechanisms

Table K.2: Interoperability-based cryptographic mechanisms

Interoperability-based cryptographic mechanism	Type of cryptographic mechanism	Characteristics / parameters	Related product function(s) / use case(s), where applicable	External specification(s) or external requirement(s)	Interoperability justification	Conditions or limitations, where applicable
<mechanism name>	<Algorithm / Primitive / Scheme / Protocol / Protocol profile / Cipher suite / Mode / Construction / Parameter set / Other>	<key length, mode, profile, cipher suite, parameter set, version, etc.>	<product function, interface, protocol context, operational context, etc.>	<external specification, regulatory requirement, mandatory public-sector requirement, operational constraint requiring use of the mechanism, technical interoperability constraint, platform compatibility requirement, etc.>	<why the mechanism is needed for interoperability>	<constraints, permitted use, excluded use, negotiation preference, external system or requirement, compensating measures, migration expectation, warning/logging, lifecycle limitation, etc.>

K.4.3 Assessment

Compliance with the requirement in clause K.4.1 is assessed in clause K.1.2.3.

NOTE: The assessment of the external specifications or external requirements themselves is outside the scope of this assessment. Their relevance is deemed confirmed by their inclusion in the present document.

Annexes L to Q:
Void

Annex R (informative): Guidance on RDPS

The clause [4.2](#) specifies the architectural component that can form a internet connected toy in scope of the present document. RDPS are typically software architectural components and in scope of the present document. The requirements specified in clause [5](#) are formulated such that they apply, where relevant, for RDPS.

For example:

- [ACM-FH] and [AUM-FH] address access control and authentication for functions whose use can cause harm, which can be provided by RDPS;
- [CONF-COM] and [INT-COM] address confidentiality and integrity of communicated data, which can be communicated from or to RDPS;
- [CONF-SSM] and [INT-SSM] address confidentiality and integrity of persistently stored data, which can be persistently stored on RDPS;
- [AVAI-TIME-OUTA-NOT] addresses a defined behaviour when time sensitive functions, which can be provided by RDPS, become or are unavailable;
- [AVAI-TIME-RECO-NETW] addresses the behaviour when a reconnection happens after the loss of network connection, which could happen for a RDPS.

History

Version	Date	Status
V1.0.0	July 2026	SRdAP process EV 20261012: 2026-07-20 to 2026-10-12