
Kibernetska varnost (CYBER) - CRA - Zahteve za kibernetsko varnost za igrače, povezane z internetom, ki jih zajema direktiva 2009/48/ES in imajo funkcije socialne interakcije (npr. govorjenje ali snemanje) ali funkcije sledenja lokaciji

Cyber Security (CYBER) - CRA - Cybersecurity requirements for Internet connected toys covered by Directive 2009/48/EC that have social interactive features (e.g. speaking or filming) or that have location tracking features

Sample Document

get full document from standards.iteh.ai

Ta slovenski standard je istoveten z: ETSI EN 304 633 V1.0.0 (2026-07)

ICS:

35.030

Informacijska varnost

IT Security

oSIST prEN 304 633 V1.0.0:2026

en

Sample Document

get full document from standards.iteh.ai

Draft ETSI EN 304 633 V1.0.0 (2026-07)



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

get full document from standards.iteh.ai

ReferenceDEN/CYBER-EUS-004

KeywordsCRA, 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-DJST]	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

Sample Document

get full document from standards.iteh.ai

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