



**Cyber Security (CYBER);
CRA;
Cybersecurity requirements for smart home products with
security functionalities;
including smart door locks, security cameras, baby monitoring
systems and alarm systems**

Reference

DEN/CYBER-EUS-0014

Keywords

CRA, cybersecurity, intelligent homes & buildings

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 authorisation 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 authorisation 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 authorises 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.....	15
3.1 Terms	15
3.1.1 Architecture related terms	15
3.1.2 Asset categories.....	15
3.1.3 Communication types.....	16
3.1.4 Data assets.....	16
3.1.5 Data related terms	18
3.1.6 Function assets	19
3.1.7 Function related terms.....	20
3.1.8 Interface	24
3.1.9 Operational environments	25
3.1.10 Use cases	25
3.1.11 Users.....	26
3.2 Symbols	26
3.3 Abbreviations.....	26
4 Product context.....	28
4.1 Product functions	28
4.1.1 Function assets	28
4.1.2 Data assets.....	29
4.2 Product architecture	30
4.3 Operational environment	31
4.3.1 General description	31
4.3.2 Physical/Hardware environment	31
4.3.3 Logical/Software environment	32
4.3.4 Connectivity aspects.....	32
4.4 Distribution of security functions	32
4.5 Users	33
4.6 Use cases.....	33
4.6.1 General	33
4.6.2 Specific use cases	33
5 Technical requirements for products.....	33
5.1 Introduction - Applicability of the requirements	33
5.2 Appropriate level of cybersecurity	34
5.2.0 Introduction on appropriate level of cybersecurity requirements	34
5.2.1 [USERNOT-NOSECFUC] User notifications on not available security functions.....	34
5.2.2 [USERNOT-SECREL] Language and representation for security-related user notifications	34
5.2.3 [GUI-SECCONF] Visual representation of security-related configuration via GUIs	34
5.2.4 [BACKUP-TRANS] Data transfer mechanisms for loss sensitive data	34
5.2.5 [BACKUP-AUTOTRANS] Automatic data transfer mechanisms for loss sensitive data	34
5.2.6 [BACKUP-EXPORT] Data export mechanisms for loss sensitive data.....	34
5.3 No known exploitable vulnerabilities	35
5.3.0 Introduction on no known exploitable vulnerabilities	35
5.3.1 [NKEV-MKAV] No known exploitable vulnerabilities	35
5.3.2 [NKEV-INIT-UDP] Initial security update before or during first use	35
5.4 Secure by default configuration	35

5.4.0	Introduction on secure by default configuration.....	35
5.4.1	[SDC-AUM-FH] Default configuration of authentication for functions whose use can cause harm	35
5.4.2	[SDC-SUM-AUTO] Default configuration of automated security updates	35
5.4.3	[SDC-SUM-NOTIF] Default configuration of update notifications	36
5.4.4	[SDC-FRM] Factory reset to restore the default state	36
5.4.5	[SDC-MON-HANDLE] Handling of events by default.....	36
5.4.6	[CRY-GENERAL] General requirements related to cryptography	36
5.4.7	[CRY-CCK-PRE-LEN] Key size of preinstalled long term confidential cryptographic keys.....	36
5.4.8	[CRY-CCK-GEN] Default key size of generated long term confidential cryptographic keys.....	36
5.4.9	[CRY-PW-PRE-COM] Complexity of preinstalled passwords	37
5.4.10	[CRY-PW-GEN-COM] Default complexity of generated passwords.....	37
5.4.11	[CRY-PW-USR-COM] Recommended complexity of user chosen passwords	37
5.5	Security updates.....	37
5.5.0	Introduction on security updates	37
5.5.1	[SU-SUPPORT] Secure software update mechanism	37
5.5.2	[SU-PROVIDE] Secure software update mechanism for core components.....	38
5.5.3	[SU-AUTO] Automated security updates	38
5.5.4	[SU-DISABLE-AUTO] Option to disable automated security updates	38
5.5.5	[SU-POSTPONE-AUTO] Option to postpone automated security updates.....	38
5.5.6	[SU-NOTIF] Update notifications.....	38
5.6	Authentication and access control	39
5.6.0	Introduction on authentication and access control	39
5.6.1	[ACM-FH] Access control for functions whose use can cause harm	39
5.6.2	[AUM-FH] Authentication for functions whose use can cause harm	39
5.6.3	[AUTHZ-LP] Least privilege in authorisation policies.....	40
5.6.4	[AUTHZ-R] Revocability of granted permissions	40
5.7	Confidentiality protection	40
5.7.0	Introduction on confidentiality protection	40
5.7.1	[CONF-SSM] Confidentiality protecting persistent storage for confidential data	40
5.7.2	[CONF-COM] Communication of confidential data.....	41
5.8	Integrity protection	41
5.8.0	Introduction on integrity protection	41
5.8.1	[INT-SSM] Integrity protecting persistent storage for integrity relevant data	41
5.8.2	[INT-COM] Communication of integrity relevant data	42
5.8.3	[INT-SWPCK] Software package verification.....	42
5.9	Data minimisation.....	43
5.9.0	Introduction on data minimisation	43
5.9.1	[DMIN-DJST] Minimise processed data.....	43
5.10	Availability protection	43
5.10.0	Introduction on availability protection	43
5.10.1	[AVAI-TIME-RECO-POW] Restoration after loss of power	43
5.10.2	[AVAI-TIME-NETW] Local operation	43
5.10.3	[AVAI-TIME-RECO-NETW] Restoration after loss of network connection	43
5.10.4	[AVAI-TIME-OUTA-NOT] Notify non-availability.....	44
5.10.5	[AVAI-TIME-PREV-NOT] Notify upcoming limitation	44
5.10.6	[AVAI-TIME-NET-PRIO] Network prioritization	44
5.10.7	[AVAI-TIME-RES-PRIO] Power resource prioritization.....	44
5.10.8	[AVAI-TIME-DOS-RATE] Incoming rate limiting	44
5.10.9	[AVAI-SUM-SCHEDULE] Scheduling of updates.....	44
5.11	Non-interference	45
5.11.0	Introduction on non-interference.....	45
5.11.1	[NOINF-AMP] Amplification control	45
5.12	Attack surface minimisation	45
5.12.0	Introduction on attack surface minimisation	45
5.12.1	[LAS-INVAL] Validation of external data input	45
5.12.2	[LAS-INSAN] Sanitisation of external data input	45
5.12.3	[LAS-PHY-INF] Only necessary physical interfaces	46
5.12.4	[LAS-LOGIC-INF] Only necessary logical interfaces active by default	46
5.12.5	[LAS-APP] Only necessary apps by default	46
5.12.6	[LAS-SBOOT] Secure boot	46
5.13	Exploit mitigation	46
5.13.0	Introduction on exploit mitigation.....	46

5.13.1	[PRIV-DATA-HIGH] Privileged access on impact class high data assets	46
5.13.2	[PRIV-FUNC-HIGH] Privileged access on impact class high function assets	46
5.14	Monitoring.....	47
5.14.0	Introduction on monitoring	47
5.14.1	[MON-LOW] Events to log for low risk SHPSF	47
5.14.2	[MON-MEDIUM] Events to log for medium risk SHPSF.....	47
5.14.3	[MON-HIGH] Events to log for high risk SHPSF	47
5.14.4	[MON-HANDLE] Handling of events.....	48
5.14.5	[LOG-TIME] Timestamps for logs	48
5.14.6	[LOG-TIME-HIGH] Real-time timestamps for logs.....	48
5.14.7	[LOG-STORE-MEDIUM] Logfile persistence for medium risk SHPSF	48
5.14.8	[LOG-STORE-HIGH] Logfile persistence for high risk SHPSF	48
5.14.9	[LOG-CONFIG] Configuration of logging mechanisms	49
5.15	Factory reset and data portability	49
5.15.0	Introduction on factory reset and data portability	49
5.15.1	[DLM-PERM] Permanent removal of user-related data	49
6	Assessment criteria for compliance with technical requirements	49
6.1	General.....	49
6.2	Appropriate level of cybersecurity.....	51
6.2.1	Assessment criteria for [USERNOT-NOSECFUC]	51
6.2.2	Assessment criteria for [USERNOT-SECREL]	51
6.2.3	Assessment criteria for [GUI-SECCONF]	52
6.2.4	Assessment criteria for [BACKUP-TRANS].....	54
6.2.5	Assessment criteria for [BACKUP-AUTOTRANS].....	55
6.2.6	Assessment criteria for [BACKUP-EXPORT].....	56
6.3	No known exploitable vulnerabilities	57
6.3.1	Assessment criteria for [NKEV-MKAV].....	57
6.3.2	Assessment criteria for [NKEV-INIT-UDP].....	59
6.4	Secure by default configuration	60
6.4.1	Assessment criteria for [SDC-AUM-FH].....	60
6.4.2	Assessment criteria for [SDC-SUM-AUTO]	61
6.4.3	Assessment criteria for [SDC-SUM-NOTIF].....	62
6.4.4	Assessment criteria for [SDC-FRM].....	63
6.4.5	Assessment criteria for [SDC-MON-HANDLE]	64
6.4.6	Assessment criteria for [CRY-GENERAL]	65
6.4.7	Assessment criteria for [CRY-CCK-PRE-LEN]	66
6.4.8	Assessment criteria for [CRY-CCK-GEN]	66
6.4.9	Assessment criteria for [CRY-PW-PRE-COM]	67
6.4.10	Assessment criteria for [CRY-PW-GEN-COM]	68
6.4.11	Assessment criteria for [CRY-PW-USR-COM].....	69
6.5	Security updates.....	71
6.5.1	Assessment criteria for [SU-SUPPORT].....	71
6.5.2	Assessment criteria for [SU-PROVIDE].....	72
6.5.3	Assessment criteria for [SU-AUTO].....	73
6.5.4	Assessment criteria for [SU-DISABLE-AUTO].....	74
6.5.5	Assessment criteria for [SU-POSTPONE-AUTO].....	75
6.5.6	Assessment criteria for [SU-NOTIF]	76
6.6	Authentication and access control	77
6.6.1	Assessment criteria for [ACM-FH].....	77
6.6.2	Assessment criteria for [AUM-FH].....	79
6.6.3	Assessment criteria for [AUTHZ-LP]	80
6.6.4	Assessment criteria for [AUTHZ-R].....	81
6.7	Confidentiality protection	82
6.7.1	Assessment criteria for [CONF-SSM]	82
6.7.2	Assessment criteria for [CONF-COM]	83
6.8	Integrity protection	84
6.8.1	Assessment criteria for [INT-SSM]	84
6.8.2	Assessment criteria for [INT-COM]	86
6.8.3	Assessment criteria for [INT-SWPCK].....	87
6.9	Data minimisation.....	88
6.9.1	Assessment criteria for [DMIN-DJST]	88

6.10	Availability protection	89
6.10.1	Assessment criteria for [AVAI-TIME-RECO-POW]	89
6.10.2	Assessment criteria for [AVAI-TIME-NETW]	91
6.10.3	Assessment criteria for [AVAI-TIME-RECO-NETW]	92
6.10.4	Assessment criteria for [AVAI-TIME-OUTA-NOT]	94
6.10.5	Assessment criteria for [AVAI-TIME-PREV-NOT]	95
6.10.6	Assessment criteria for [AVAI-TIME-NET-PRIO]	97
6.10.7	Assessment criteria for [AVAI-TIME-RES-PRIO]	98
6.10.8	Assessment criteria for [AVAI-TIME-DOS-RATE]	99
6.10.9	Assessment criteria for [AVAI-SUM-SCHEDULE]	100
6.11	Non-interference	101
6.11.1	Assessment criteria for [NOINF-AMP]	101
6.12	Attack surface minimisation	102
6.12.1	Assessment criteria for [LAS-INVAL]	102
6.12.2	Assessment criteria for [LAS-INSAN]	103
6.12.3	Assessment criteria for [LAS-PHY-INF]	104
6.12.4	Assessment criteria for [LAS-LOGIC-INF]	105
6.12.5	Assessment criteria for [LAS-APP]	106
6.12.6	Assessment criteria for [LAS-SBOOT]	107
6.13	Exploit mitigation	108
6.13.1	Assessment criteria for [PRIV-DATA-HIGH]	108
6.13.2	Assessment criteria for [PRIV-FUNC-HIGH]	109
6.14	Monitoring	110
6.14.1	Assessment criteria for [MON-LOW]	110
6.14.2	Assessment criteria for [MON-MEDIUM]	111
6.14.3	Assessment criteria for [MON-HIGH]	112
6.14.4	Assessment criteria for [MON-HANDLE]	113
6.14.5	Assessment criteria for [LOG-TIME]	114
6.14.6	Assessment criteria for [LOG-TIME-HIGH]	115
6.14.7	Assessment criteria for [LOG-STORE-MEDIUM]	116
6.14.8	Assessment criteria for [LOG-STORE-HIGH]	117
6.14.9	Assessment criteria for [LOG-CONFIG]	118
6.15	Factory reset and data portability	119
6.15.1	Assessment criteria for [DLM-PERM]	119

Annex A (informative):	Relationship between the present document and the essential cybersecurity requirements of EU Regulation 2024/2847	122
-------------------------------	--	------------

Annex B (informative):	Security analysis.....	127
-------------------------------	-------------------------------	------------

B.1	General	127
B.2	Assets	127
B.3	Risk factors.....	127
B.4	Assumptions	127
B.5	Threats	128
B.6	Relationship between the present document and the covered/not covered cybersecurity risks	128
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	142
Annex E (normative):	Protection measures.....	149
E.1	Authentication mechanism strength	149
E.1.1	[AUM-FH] Authentication for functions whose use can cause harm	149
E.1.1.1	General	149
E.1.1.2	[AUM-E-I-Basic] AUTH.Basic inheritance based SFA	149
E.1.1.3	[AUM-E-K-Basic] AUTH.Basic knowledge based SFA	149
E.1.1.4	[AUM-E-I-Normal] AUTH.Normal inheritance based SFA	149
E.1.1.5	[AUM-E-K-Normal] AUTH.Normal knowledge based SFA	149
E.1.1.6	[AUM-E-P-Normal] AUTH.Normal possession based SFA	149
E.1.1.7	[AUM-E-MFA-Normal] AUTH.Normal MFA	150
E.1.1.8	[AUM-E-I-Enhanced] AUTH.Enhanced inheritance based SFA	150
E.1.1.9	[AUM-E-K-Enhanced] AUTH.Enhanced knowledge based SFA	150
E.1.1.10	[AUM-E-P-Enhanced] AUTH.Enhanced possession based SFA	150
E.1.1.11	[AUM-E-MFA-Enhanced] AUTH.Enhanced MFA	151
E.1.1.12	[AUM-E-I-Strong] AUTH.Strong inheritance based SFA	151
E.1.1.13	[AUM-E-P-Strong] AUTH.Strong possession based SFA	151
E.1.1.14	[AUM-E-MFA-Strong] AUTH.Strong MFA	151
E.1.1.15	[AUM-E-Replay] AUTH.Normal, AUTH.Enhanced and AUTH.Strong replay protection	151
E.1.1.16	[AUM-E-PitM] AUTH.Normal, AUTH.Enhanced and AUTH.Strong person in the middle protection	152
E.1.2	Assessment for [AUM-FH] authentication mechanism strength	152
E.1.2.1	General	152
E.1.2.2	Assessment criteria for [AUM-E-I-Basic]	152
E.1.2.3	Assessment criteria for [AUM-E-K-Basic]	153
E.1.2.4	Assessment criteria for [AUM-E-I-Normal]	154
E.1.2.5	Assessment criteria for [AUM-E-K-Normal]	155
E.1.2.6	Assessment criteria for [AUM-E-P-Normal]	155
E.1.2.7	Assessment criteria for [AUM-E-MFA-Normal]	157
E.1.2.8	Assessment criteria for [AUM-E-I-Enhanced]	158
E.1.2.9	Assessment criteria for [AUM-E-K-Enhanced]	159
E.1.2.10	Assessment criteria for [AUM-E-P-Enhanced]	160
E.1.2.11	Assessment criteria for [AUM-E-MFA-Enhanced]	162
E.1.2.12	Assessment criteria for [AUM-E-I-Strong]	163
E.1.2.13	Assessment criteria for [AUM-E-P-Strong]	164
E.1.2.14	Assessment criteria for [AUM-E-MFA-Strong]	165
E.1.2.15	Assessment criteria for [AUM-E-Replay]	166
E.1.2.16	Assessment criteria for [AUM-E-PitM]	167
E.2	Integrity protection strength	168
E.2.1	[INT-SSM] Integrity protecting persistent storage for integrity relevant data	168
E.2.1.1	General	168
E.2.1.2	[INT-SSM-E-Basic] INT.SSM.Basic integrity protecting secure storage mechanism	168
E.2.1.3	[INT-SSM-E-Normal] INT.SSM.Normal integrity protecting secure storage mechanism	169
E.2.1.4	[INT-SSM-E-Enhanced] INT.SSM.Enhanced integrity protecting secure storage mechanism	169
E.2.1.5	[INT-SSM-E-Strong] INT.SSM.Strong integrity protecting secure storage mechanism	169
E.2.2	Assessment for integrity protecting secure storage mechanism strength	169
E.2.2.1	General	169
E.2.2.2	Assessment criteria for [INT-SSM-E-Basic]	169
E.2.2.3	Assessment criteria for [INT-SSM-E-Normal]	170
E.2.2.4	Assessment criteria for [INT-SSM-E-Enhanced]	171
E.2.2.5	Assessment criteria for [INT-SSM-E-Strong]	172
E.2.3	[INT-COM] Communication of integrity relevant data	173
E.2.3.1	General	173
E.2.3.2	[INT-COM-E-Basic] INT.COM.Basic integrity protecting communication mechanism	173
E.2.3.3	[INT-COM-E-Normal] INT.COM.Normal integrity protecting communication mechanism	173
E.2.3.4	[INT-COM-E-Enhanced] INT.COM.Enhanced integrity protecting communication mechanism	173
E.2.3.5	[INT-COM-E-EndAuth] INT.COM.Normal and INT.COM.Enhanced integrity protecting communication mechanism endpoint authentication	174

E.2.3.6	[INT-COM-E-Downgrade] INT.COM.Normal and INT.COM.Enhanced integrity protecting communication mechanism downgrade protection	174
E.2.4	Assessment for integrity protecting communication mechanism strength	174
E.2.4.1	General	174
E.2.4.2	Assessment criteria for [INT-COM-E-Basic]	174
E.2.4.3	Assessment criteria for [INT-COM-E-Normal]	175
E.2.4.4	Assessment criteria for [INT-COM-E-Enhanced]	176
E.2.4.5	Assessment criteria for [INT-COM-E-EndAuth]	177
E.2.4.6	Assessment criteria for [INT-COM-E-Downgrade]	178
E.2.5	[INT-SWPCK] Software package verification	179
E.2.5.1	General	179
E.2.5.2	[INT-SWPCK-E-Basic] INT.SW.VER.Basic software package verification mechanism	179
E.2.5.3	[INT-SWPCK-E-Normal] INT.SW.VER.Normal software package verification mechanism	179
E.2.5.4	[INT-SWPCK-E-Enhanced] INT.SW.VER.Enhanced software package verification mechanism	180
E.2.6	Assessment for integrity protecting communication mechanism strength	180
E.2.6.1	General	180
E.2.6.2	Assessment criteria for [INT-SWPCK-E-Basic]	180
E.2.6.3	Assessment criteria for [INT-SWPCK-E-Normal]	181
E.2.6.4	Assessment criteria for [INT-SWPCK-E-Enhanced]	182
E.3	Confidentiality protection strength	183
E.3.1	[CONF-SSM] Confidentiality protecting persistent storage for confidential data	183
E.3.1.1	General	183
E.3.1.2	[CONF-SSM-E-Basic] CONF.SSM.Basic confidentiality protecting secure storage mechanism	183
E.3.1.3	[CONF-SSM-E-Normal] CONF.SSM.Normal confidentiality protecting secure storage mechanism	183
E.3.1.4	[CONF-SSM-E-Enhanced] CONF.SSM.Enhanced confidentiality protecting secure storage mechanism	184
E.3.1.5	[CONF-SSM-E-Strong] CONF.SSM.Strong confidentiality protecting secure storage mechanism	184
E.3.2	Assessment for integrity protecting secure storage mechanism strength	184
E.3.2.1	General	184
E.3.2.2	Assessment criteria for [CONF-SSM-E-Basic]	184
E.3.2.3	Assessment criteria for [CONF-SSM-E-Normal]	185
E.3.2.4	Assessment criteria for [CONF-SSM-E-Enhanced]	186
E.3.2.5	Assessment criteria for [CONF-SSM-E-Strong]	187
E.3.3	[CONF-COM] Communication of confidential data	188
E.3.3.1	General	188
E.3.3.2	[CONF-COM-E-Basic] CONF.COM.Basic confidentiality protecting communication mechanism	188
E.3.3.3	[CONF-COM-E-Normal] CONF.COM.Normal confidentiality protecting communication mechanism	188
E.3.3.4	[CONF-COM-E-Enhanced] CONF.COM.Enhanced confidentiality protecting communication mechanism	188
E.3.3.5	[CONF-COM-E-EndAuth] CONF.COM.Normal and CONF.COM.Enhanced confidentiality protecting communication mechanism endpoint authentication	189
E.3.3.6	[CONF-COM-E-Downgrade] CONF.COM.Normal and CONF.COM.Enhanced confidentiality protecting communication mechanism downgrade protection	189
E.3.4	Assessment for confidentiality protecting communication mechanism strength	189
E.3.4.1	General	189
E.3.4.2	Assessment criteria for [CONF-COM-E-Basic]	189
E.3.4.3	Assessment criteria for [CONF-COM-E-Normal]	190
E.3.4.4	Assessment criteria for [CONF-COM-E-Enhanced]	191
E.3.4.5	Assessment criteria for [CONF-COM-E-EndAuth]	192
E.3.4.6	Assessment criteria for [CONF-COM-E-Downgrade]	193

Annex F (informative): Guidance for the application of the present document195

Annex G: Void198

Annex H (informative): Mapping of specific use-case assets with the data and function assets covered by this European standard199

H.1 General199

H.2 Terminology mappings for building intercom systems (BIS)199

H.3	Terminology mappings for fire/gas detection device/systems (FGS)	200
H.4	Terminology mappings for intrusion and hold-up alarm systems (I&HAS).....	201
H.5	Terminology mappings for social alarm systems (SAS).....	202
Annexes I to J: Void		206
Annex K (normative): Generic cryptographic requirements and assessment.....		207
K.1	Cryptography.....	207
K.1.1	[CRY-SOTA] Requirement	207
K.1.2	Assessment criteria	208
K.1.2.1	Assessment criteria for [CRY-SOTA] concerning ACM-listed cryptographic mechanisms	208
K.1.2.2	Assessment criteria for [CRY-SOTA] concerning ACM-extended cryptographic mechanisms.....	209
K.1.2.3	Assessment criteria for [CRY-SOTA] concerning interoperability-based cryptographic mechanisms ...	210
K.2	Crypto agility	211
K.2.1	[CRY-AGIL] Requirement	211
K.2.2	Assessment criteria for [CRY-AGIL].....	212
K.3	ACM-extended cryptographic mechanisms	213
K.3.1	[CRY-ACM-EXT] Requirement	213
K.3.2	List of ACM-extended cryptographic mechanisms	214
K.3.3	Assessment	214
K.4	Interoperability-based cryptographic mechanisms.....	214
K.4.1	[CRY-INTOP] Requirement	214
K.4.2	List of interoperability-based cryptographic mechanisms	215
K.4.3	Assessment	215
Annexes L to Q: Void		216
Annex R (informative): Guidance on RDPS		217
History		218

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 M/606 - C(2025)618 [i.3] final 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.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 [4](#) also defines specific use cases.
- 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 [H](#) provides a mapping of the terminology used in the context of other existing standards related to the specific use cases with the data assets and function assets defined and used in 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 smart home products with security functionalities related to cybersecurity. The products with digital elements in scope, thereafter "smart home products with security functionalities":

- are specified within the "technical description" of the "category of product" number "17." by the Commission Implementing Regulation (EU) 2025/2392 [i.2] as:
"Products with digital elements that protect the physical security of consumers in a residential setting and which can be controlled or managed remotely from other systems, as well as hardware and software that centrally control such products.
This category includes but is not limited to smart door locking devices, baby monitoring systems, alarm systems and home security cameras"; 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], Annex I, Part I under the conditions identified in clause 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](#) 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 - 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](#): "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] IEC 62820-1-1:2026: "Building intercom systems - Part 1-1: System requirements - General".
- [i.15] IEC 62820-1-2:2017: "Building intercom systems - Part 1-2: System requirements - Building intercom systems using the internet protocol (IP)".
- [i.16] IEC 62820-2:2017: "Building intercom systems - Part 2: Requirements for advanced security building intercom systems (ASBIS)".
- [i.17] IEC 62820-3-1:2017: "Building intercom systems - Part 3-1: Application guidelines - General".
- [i.18] IEC 62820-3-2:2018: "Building intercom systems - Part 3-2: Application guidelines - Advanced security building intercom systems (ASBIS)".
- [i.19] EN 14604: "Smoke alarm devices" produced by CEN CENELEC.
- [i.20] BS 5446-2:2003: "Fire detection and fire alarm devices for dwellings Specification for heat alarms".
- [i.21] EN 50291-1: "Gas detectors - Electrical apparatus for the detection of carbon monoxide in domestic premises - Part 1: Test methods and performance requirements" produced by CEN CENELEC.
- [i.22] EN 50194-1: "Electrical apparatus for the detection of flammable gases in household premises - Part 1: Test methods and performance requirements" produced by CEN CENELEC.
- [i.23] EN 50131-1: "Alarm systems - Intrusion and hold-up systems - System requirements" produced by CEN CENELEC.
- [i.24] EN 50131-2-2: "Alarm systems - Intrusion and hold-up systems - Requirements for passive infrared detectors" produced by CEN CENELEC.

- [i.25] EN 50131-2-3: "Alarm systems - Intrusion and hold-up systems - Requirements for microwave detectors" produced by CEN CENELEC.
- [i.26] EN 50131-2-4: "Alarm systems - Intrusion and hold-up systems - Requirements for combined passive infrared and microwave detectors" produced by CEN CENELEC.
- [i.27] EN 50131-2-5: "Alarm systems - Intrusion and hold-up systems - Requirements for combined passive infrared and ultrasonic detectors" produced by CEN CENELEC.
- [i.28] EN 50131-2-6: "Alarm systems - Intrusion and hold-up systems - Opening contacts (magnetic)" produced by CEN CENELEC.
- [i.29] EN 50131-2-7-1: "Alarm systems - Intrusion and hold-up systems - Intrusion detectors - Glass break detectors (acoustic)" produced by CEN CENELEC.
- [i.30] EN 50131-2-7-2: "Alarm systems - Intrusion and hold-up systems - Intrusion detectors - Glass break detectors (passive)" produced by CEN CENELEC.
- [i.31] EN 50131-2-7-3: "Alarm systems - Intrusion and hold-up systems - Intrusion detectors - Glass break detectors (active)" produced by CEN CENELEC.
- [i.32] EN 50131-2-8: "Alarm systems - Intrusion and hold-up systems - Intrusion detectors - Shock detectors" produced by CEN CENELEC.
- [i.33] EN 50131-2-10: "Alarm systems - Intrusion and hold-up systems - Intrusion detectors - Lock state contacts (magnetic)" produced by CEN CENELEC.
- [i.34] EN 50131-3: "Alarm systems - Intrusion and hold-up systems - Control and indicating equipment" produced by CEN CENELEC.
- [i.35] EN 50131-4: "Alarm systems - Intrusion and hold-up systems - Warning devices" produced by CEN CENELEC.
- [i.36] EN 50131-5-3: "Alarm systems - Intrusion systems - Requirements for interconnections equipment using radio frequency techniques" produced by CEN CENELEC.
- [i.37] EN 50131-6: "Alarm systems - Intrusion and hold-up systems - Power supplies" produced by CEN CENELEC.
- [i.38] EN 50131-8: "Alarm systems - Intrusion and hold-up systems - Security fog devices" produced by CEN CENELEC.
- [i.39] EN 50131-10: "Alarm systems - Intrusion and hold-up systems - Application specific requirements for Supervised Premises Transceiver (SPT)" produced by CEN CENELEC.
- [i.40] EN 50131-13: "Alarm systems - Intrusion and hold-up systems - Pyrotechnic Obscuration Security Devices" produced by CEN CENELEC.
- [i.41] EN 50134-1: "Alarm systems - Social alarm systems - System requirements" produced by CEN CENELEC.
- [i.42] EN 50134-2: "Alarm systems - Social alarm systems - Trigger devices" produced by CEN CENELEC.
- [i.43] EN 50134-3: "Alarm systems - Social alarm systems - Local unit and controller" produced by CEN CENELEC.
- [i.44] EN 50134-5: "Alarm systems - Social alarm systems - Interconnections and communications" produced by CEN CENELEC.
- [i.45] EN 50134-7: "Alarm systems - Social alarm systems - Application guidelines" produced by CEN CENELEC.
- [i.46] [NIST FIPS 203](#): "Module-Lattice-Based Key-Encapsulation Mechanism Standard".
- [i.47] [NIST FIPS 204](#): "Module-Lattice-Based Digital Signature Standard".

[i.48] [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 SHPSF-oriented functional tasks on a device, operating on top of the core software, and without direct responsibility for hardware initialization 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 SHPSF

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 SHPSF including its associated software architectural component

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

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 SHPSF

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

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