



**Cyber Security (CYBER);
CRA;
Cybersecurity requirements for personal wearable**

get full document from standards.iteh.ai

ReferenceDEN/CYBER-EUS-003

KeywordsCRA, cybersecurity, wearable

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
3.2 Symbols.....	17
3.3 Abbreviations	17
4 Product context.....	19
4.0 Introduction	19
4.0.1 General.....	19
4.0.2 Personal wearable that have a health monitoring purpose	20
4.0.3 Personal wearable that are intended for the use by and for children.....	20
4.1 Product functions.....	20
4.1.0 Introduction.....	20
4.1.1 Health monitoring functionalities (essential functionalities)	20
4.1.2 Location-based functionalities (essential functionalities)	21
4.1.3 Parental Control (essential functionalities).....	21
4.1.4 Notification functionalities (essential functionalities)	22
4.1.5 Input commands from user or other connected devices (supporting functionalities).....	22
4.1.6 Data monitoring and storage (supporting functionalities).....	22
4.1.7 General functionalities (supporting functionalities).....	22
4.1.8 Summary of the personal wearable functions	22
4.1.9 Data assets	23
4.2 Product Architecture.....	24
4.2.0 Introduction.....	24
4.2.1 Personal wearable that have a health monitoring purpose architecture	24
4.2.2 Personal wearable that are intended for the use by and for children architecture	25
4.3 Operational Environment	27
4.3.1 General description	27
4.3.2 Physical operational environment.....	27
4.3.3 Logical operational environment	27
4.3.4 Connectivity aspects	27
4.4 Distribution of Security Functions	28
4.5 Users.....	28
4.5.1 End-Users	28
4.5.2 Manufacturers	28
4.6 Use cases	29
5 Technical requirements for personal wearables	29
5.1 Introduction - Applicability of the requirements	29
5.2 Appropriate level of cybersecurity	29
5.2.0 Appropriate level of cybersecurity introduction	29
5.2.1 [USERNOT-NOSECFUC] User notifications on not available security functions	29
5.2.2 [USERNOT-SECREL] Language and representation for security-related user notifications.....	29
5.2.3 [GUI-SECCONF] Visual representation of security-related configuration via GUIs.....	29
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.....	30

5.3.0	No known exploitable vulnerabilities introduction.....	30
5.3.1	[NKEV-MKAV] No known exploitable vulnerabilities	30
5.3.2	[NKEV-INIT-UPD] Initial security update before or during first use	30
5.4	Secure by default configuration.....	31
5.4.0	Secure by default configuration introduction.....	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.....	31
5.4.3	[SDC-SUM-NOTIF] Default configuration of update notifications.....	31
5.4.4	[SDC-FRM] Factory reset to restore the default state.....	31
5.4.5	[SDC-PARCONT] Default configuration for parental control	32
5.4.6	[SDC-MON-HANDLE] Handling of events by default	32
5.4.7	[CRY-SOTA] State-of-the-art cryptography	32
5.4.8	[CRY-CCK-PRE-LEN] Key size of preinstalled confidential cryptographic keys	32
5.4.9	[CRY-CCK-GEN] Default key size of generated confidential cryptographic keys.....	32
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.....	33
5.5	Security updates	33
5.5.0	Security updates introduction	33
5.5.1	[SU-SUPPORT] Software update mechanism.....	33
5.5.2	[SU-PROVIDE] Secure software update mechanism for core components	33
5.5.3	[SU-AUTO] Automated security updates.....	34
5.5.4	[SU-DISABLE-AUTO] Option to disable automated security updates	34
5.5.5	[SU-POSTPONE-AUTO] Option to postpone automated security updates	34
5.5.6	[SU-NOTIF] Update notifications	34
5.6	Authentication and access control	34
5.6.0	Authentication and access control introduction	34
5.6.1	[ACM-FH] Access control for functions whose use can cause harm	34
5.6.2	[AUM-FH] Authentication for functions whose use can cause harm	35
5.6.3	[AUTHZ-LP] Least privilege in authorisation policies	36
5.6.4	[AUTHZ-R] Revocability of granted permissions.....	36
5.6.5	[PARCONT] Support of parental control	36
5.6.6	[AUTHZ-PC] Authorisation policies for parental control	37
5.7	Confidentiality protection.....	37
5.7.0	Confidentiality protection introduction.....	37
5.7.1	[CONF-SSM] Confidentiality protecting persistent storage for confidential data.....	37
5.7.2	[CONF-COM] Communication of confidential data	37
5.7.3	[CONF-MON-HW] Indication of active capture of audio or video data	38
5.8	Integrity protection	38
5.8.0	Integrity protection introduction	38
5.8.1	[INT-SSM] Integrity protecting persistent storage for integrity relevant data.....	38
5.8.2	[INT-SWPCK] Software package verification	39
5.8.3	[INT-COM] Communication of integrity relevant data.....	39
5.9	Data minimisation	40
5.9.0	Data minimisation introduction	40
5.9.1	[DMIN-DJST] Documented justification of processed data.....	40
5.10	Availability protection.....	40
5.10.0	Availability protection introduction.....	40
5.10.1	[AVAI-TIME-RECO-POW] Restoration after loss of power.....	40
5.10.2	[AVAI-TIME-NETW] Local operation.....	40
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-PREV-PRIO] Network prioritisation	41
5.10.7	[AVAI-TIME-RES-PRIO] Power resource prioritisation.....	41
5.10.8	[AVAI-UPD-SCHEDULE] Scheduling of updates	42
5.11	Non-interference.....	42
5.12	Attack surface minimisation.....	42
5.12.0	Attack surface minimisation introduction.....	42
5.12.1	[LAS-INVAL] Validation of external data input.....	42
5.12.2	[LAS-INSAN] Sanitisation of external data input	42
5.12.3	[LAS-PHY-INF] Only necessary physical interfaces	42

5.12.4	[LAS-LOGIC-INF] Only necessary logical interfaces active by default.....	43
5.12.5	[LAS-SBOOT] Secure boot.....	43
5.13	Exploit mitigation.....	43
5.13.0	Exploit mitigation introduction.....	43
5.13.1	[PRIV-DATA-HIGH] Privileged access on impact class high data assets	43
5.13.2	[PRIV-FUNC-HIGH] Privileged access on impact class high function assets.....	43
5.14	Monitoring.....	43
5.14.0	Monitoring introduction.....	43
5.14.1	[MON-LOW] Events to log for low risk personal wearable.....	44
5.14.2	[MON-MEDIUM] Events to log for medium risk personal wearable	44
5.14.3	[MON-HIGH] Events to log for high risk personal wearable.....	44
5.14.4	[MON-HANDLE] Handling of events	44
5.14.5	[LOG-TIME] Timestamps for logs.....	44
5.14.6	[LOG-TIME-HIGH] Real-time timestamps for logs	44
5.14.7	[LOG-STORE-MEDIUM] Logfile persistence for medium risk personal wearable	45
5.14.8	[LOG-STORE-HIGH] Logfile persistence for high risk personal wearable.....	45
5.14.9	[LOG-CONFIG] Configuration of logging mechanisms.....	45
5.15	Factory reset and data portability	45
5.15.0	Factory reset and data portability introduction	45
5.15.1	[DLM-PERM] Permanent removal of user-related data	46
6	Assessment criteria for compliance with technical requirements	46
6.1	Introduction to the assessment and compliance criteria	46
6.2	Appropriate level of cybersecurity	47
6.2.1	Assessment criteria for [USERNOT-NOSECFUC].....	47
6.2.2	Assessment criteria for [USERNOT-SECREL].....	48
6.2.3	Assessment criteria for [GUI-SECCONF].....	49
6.2.4	Assessment criteria for [BACKUP-TRANS].....	50
6.2.5	Assessment criteria for [BACKUP-AUTOTRANS]	51
6.2.6	Assessment criteria for [BACKUP-EXPORT]	52
6.3	No known exploitable vulnerabilities.....	54
6.3.1	Assessment criteria for [NKEV-MKAV]	54
6.3.2	Assessment criteria for [NKEV-INIT-UPD]	55
6.4	Secure by default configuration.....	56
6.4.1	Assessment criteria for [SDC-AUM-FH]	56
6.4.2	Assessment criteria for [SDC-SUM-AUTO].....	57
6.4.3	Assessment criteria for [SDC-SUM-NOTIF]	58
6.4.4	Assessment criteria for [SDC-FRM]	59
6.4.5	Assessment criteria for [SDC-PARCONT]	60
6.4.6	Assessment criteria for [SDC-MON-HANDLE]	61
6.4.7	Assessment criteria for [CRY-SOTA].....	62
6.4.8	Assessment criteria for [CRY-CCK-PRE-LEN].....	62
6.4.9	Assessment criteria for [CRY-CCK-GEN].....	63
6.4.10	Assessment criteria for [CRY-PW-PRE-COM].....	64
6.4.11	Assessment criteria for [CRY-PW-GEN-COM].....	65
6.4.12	Assessment criteria for [CRY-PW-USR-COM]	66
6.5	Security updates	67
6.5.1	Assessment criteria for [SU-SUPPORT]	67
6.5.2	Assessment criteria for [SU-PROVIDE]	68
6.5.3	Assessment criteria for [SU-AUTO].....	69
6.5.4	Assessment criteria for [SU-DISABLE-AUTO]	70
6.5.5	Assessment criteria for [SU-POSTPONE-AUTO]	71
6.5.6	Assessment criteria for [SU-NOTIF].....	72
6.6	Authentication and access control.....	73
6.6.1	Assessment criteria for [ACM-FH]	73
6.6.2	Assessment criteria for [AUM-FH]	75
6.6.3	Assessment criteria for [AUTHZ-LP].....	76
6.6.4	Assessment criteria for [AUTHZ-R].....	76
6.6.5	Assessment criteria for [PARCONT]	77
6.6.6	Assessment criteria for [AUTHZ-PC]	78
6.7	Confidentiality protection.....	79
6.7.1	Assessment criteria for [CONF-SSM].....	79

6.7.2	Assessment criteria for [CONF-COM]	80
6.7.3	Assessment criteria for [CONF-MON-HW]	82
6.8	Integrity protection	83
6.8.1	Assessment criteria for [INT-SSM]	83
6.8.2	Assessment criteria for [INT-SWPCK]	84
6.8.3	Assessment criteria for [INT-COM]	85
6.9	Data minimisation	87
6.9.1	Assessment criteria for [DMIN-DJST]	87
6.10	Availability protection	87
6.10.1	Assessment criteria for [AVAI-TIME-RECO-POW]	87
6.10.2	Assessment criteria for [AVAI-TIME-NETW]	89
6.10.3	Assessment criteria for [AVAI-TIME-RECO-NETW]	90
6.10.4	Assessment criteria for [AVAI-TIME-OUTA-NOT]	92
6.10.5	Assessment criteria for [AVAI-TIME-PREV-NOT]	93
6.10.6	Assessment criteria for [AVAI-TIME-RES-PRIO]	95
6.10.7	Assessment criteria for [AVAI-TIME-RES-PRIO]	96
6.10.8	Assessment criteria for [AVAI-SUM-SCHEDULE]	97
6.11	Non-interference	98
6.12	Attack surface minimisation	98
6.12.1	Assessment criteria for [LAS-INVAL]	98
6.12.2	Assessment criteria for [LAS-INSAN]	99
6.12.3	Assessment criteria for [LAS-PHY-INF]	100
6.12.4	Assessment criteria for [LAS-LOGIC-INF]	101
6.12.5	Assessment criteria for [LAS-SBOOT]	102
6.13	Exploit mitigation	103
6.13.1	Assessment criteria for [PRIV-DATA-HIGH]	103
6.13.2	Assessment criteria for [PRIV-FUNC-HIGH]	104
6.14	Monitoring	105
6.14.1	Assessment criteria for [MON-LOW]	105
6.14.2	Assessment criteria for [MON-MEDIUM]	106
6.14.3	Assessment criteria for [MON-HIGH]	106
6.14.4	Assessment criteria for [MON-HANDLE]	107
6.14.5	Assessment criteria for [LOG-TIME]	108
6.14.6	Assessment criteria for [LOG-TIME-HIGH]	109
6.14.7	Assessment criteria for [LOG-STORE-MEDIUM]	110
6.14.8	Assessment criteria for [LOG-STORE-HIGH]	111
6.14.9	Assessment criteria for [LOG-CONFIG]	112
6.15	Factory reset and data portability	114
6.15.1	Assessment criteria for [DLM-PERM]	114

Annex A (informative):	Relationship between the present document and the requirements of EU Regulation 2024/2847	116
-------------------------------	--	------------

Annex B (informative):	Security analysis	121
-------------------------------	--------------------------------	------------

B.1	General	121
B.2	Assets	121
B.3	Risk factors	121
B.4	Assumptions	121
B.5	Threats	122
B.6	Relationship between the present document and the covered/not covered cybersecurity risks	122
B.7	Guidance for determining impact classes	126
B.7.1	General	126
B.7.2	Confidential data	126
B.7.3	loss sensitive data	127
B.7.4	time sensitive data and time sensitive function	127
B.7.5	integrity relevant data and integrity relevant function	127

Annex C:	Void	129
-----------------	-------------------	------------

Annex D (normative):	Relationship between specific data and functions assets covered by the present document to impact classes for generic asset categories.....	130
D.1	Data assets	130
D.2	Function assets	131
D.2.1	Functions	131
D.2.2	Functions whose use can cause harm	131
Annex E (normative):	Protection measures.....	133
E.1	authentication mechanism strength	133
E.1.1	[AUM-FH] Authentication for functions whose use can cause harm.....	133
E.1.1.1	General.....	133
E.1.1.2	[AUM-E-I-Basic] AUTH.Basic inheritance based SFA	133
E.1.1.3	[AUM-E-K-Basic] AUTH.Basic knowledge based SFA.....	133
E.1.1.4	[AUM-E-I-Medium] AUTH.Medium inheritance based SFA	133
E.1.1.5	[AUM-E-K-Medium] AUTH.Medium knowledge based SFA	133
E.1.1.6	[AUM-E-P-Medium] AUTH.Medium possession based SFA	133
E.1.1.7	[AUM-E-MFA-Medium] AUTH.Medium MFA.....	134
E.1.1.8	[AUM-E-I-Enhanced] AUTH.Enhanced inheritance based SFA.....	134
E.1.1.9	[AUM-E-K-Enhanced] AUTH.Enhanced knowledge based SFA	134
E.1.1.10	[AUM-E-P-Enhanced] AUTH.Enhanced possession based SFA	134
E.1.1.11	[AUM-E-MFA-Enhanced] AUTH.Enhanced MFA	135
E.1.1.12	[AUM-E-I-Strong] AUTH.Strong inheritance based SFA.....	135
E.1.1.13	[AUM-E-P-Strong] AUTH.Strong possession based SFA	135
E.1.1.14	[AUM-E-MFA-Strong] AUTH.Strong MFA	135
E.1.1.15	[AUM-E-Replay] AUTH.Medium, AUTH.Enhanced and AUTH.Strong replay protection.....	135
E.1.1.16	[AUM-E-PitM] AUTH.Medium, AUTH.Enhanced and AUTH.Strong person in the middle protection	136
E.1.2	Assessment for [AUM-FH] authentication mechanism strength.....	136
E.1.2.1	General.....	136
E.1.2.2	Assessment criteria for [AUM-E-I-Basic]	136
E.1.2.3	Assessment criteria for [AUM-E-K-Basic].....	137
E.1.2.4	Assessment criteria for [AUM-E-I-Medium].....	138
E.1.2.5	Assessment criteria for [AUM-E-K-Medium]	138
E.1.2.6	Assessment criteria for [AUM-E-P-Medium].....	139
E.1.2.7	Assessment criteria for [AUM-E-MFA-Medium]	140
E.1.2.8	Assessment criteria for [AUM-E-I-Enhanced]	141
E.1.2.9	Assessment criteria for [AUM-E-K-Enhanced].....	142
E.1.2.10	Assessment criteria for [AUM-E-P-Enhanced]	143
E.1.2.11	Assessment criteria for [AUM-E-MFA-Enhanced]	145
E.1.2.12	Assessment criteria for [AUM-E-I-Strong]	146
E.1.2.13	Assessment criteria for [AUM-E-P-Strong]	147
E.1.2.14	Assessment criteria for [AUM-E-MFA-Strong]	148
E.1.2.15	Assessment criteria for [AUM-E-Replay]	149
E.1.2.16	Assessment criteria for [AUM-E-PitM].....	150
E.2	integrity protection strength	151
E.2.1	[INT-SSM] Integrity protecting persistent storage for integrity relevant data	151
E.2.1.1	General.....	151
E.2.1.2	[INT-SSM-E-Basic] INT.SSM.Basic integrity protecting secure storage mechanism	151
E.2.1.3	[INT-SSM-E-Medium] INT.SSM.Medium integrity protecting secure storage mechanism	152
E.2.1.4	[INT-SSM-E-Enhanced] INT.SSM.Enhanced integrity protecting secure storage mechanism.....	152
E.2.1.5	[INT-SSM-E-Strong] INT.SSM.Strong integrity protecting secure storage mechanism.....	152
E.2.2	Assessment for integrity protecting secure storage mechanism strength	152
E.2.2.1	General.....	152
E.2.2.2	Assessment criteria for [INT-SSM-E-Basic]	152
E.2.2.3	Assessment criteria for [INT-SSM-E-Medium].....	153
E.2.2.4	Assessment criteria for [INT-SSM-E-Enhanced]	154
E.2.2.5	Assessment criteria for [INT-SSM-E-Strong]	155
E.2.3	[INT-COM] Communication of integrity relevant data	156
E.2.3.1	General.....	156

E.2.3.2	[INT-COM-E-Basic] INT.COM.Basic integrity protecting communication mechanism.....	156
E.2.3.3	[INT-COM-E-Medium] INT.COM.Medium integrity protecting communication mechanism.....	156
E.2.3.4	[INT-COM-E-Enhanced] INT.COM.Enhanced integrity protecting communication mechanism	156
E.2.3.5	[INT-COM-E-EndAuth] INT.COM.Medium and INT.COM.Enhanced integrity protecting communication mechanism endpoint authentication.....	156
E.2.3.6	[INT-COM-E-Downgrade] INT.COM.Medium and INT.COM.Enhanced integrity protecting communication mechanism downgrade protection.....	157
E.2.4	Assessment for integrity protecting communication mechanism strength	157
E.2.4.1	General.....	157
E.2.4.2	Assessment criteria for [INT-COM-E-Basic]	157
E.2.4.3	Assessment criteria for [INT-COM-E-Medium]	158
E.2.4.4	Assessment criteria for [INT-COM-E-Enhanced]	159
E.2.4.5	Assessment criteria for [INT-COM-E-EndAuth].....	160
E.2.4.6	Assessment criteria for [INT-COM-E-Downgrade]	161
E.2.5	[INT-SWPCK] Software package verification.....	162
E.2.5.1	General.....	162
E.2.5.2	[INT-SWPCK-E-Basic] INT.SW.VER.Basic software package verification mechanism.....	162
E.2.5.3	[INT-SWPCK-E-Medium] INT.SW.VER.Medium software package verification mechanism	162
E.2.5.4	[INT-SWPCK-E-Enhanced] INT.SW.VER.Enhanced software package verification mechanism	162
E.2.6	Assessment for integrity protecting communication mechanism strength	162
E.2.6.1	General.....	162
E.2.6.2	Assessment criteria for [INT-SWPCK-E-Basic]	162
E.2.6.3	Assessment criteria for [INT-SWPCK-E-Medium].....	163
E.2.6.4	Assessment criteria for [INT-SWPCK-E-Enhanced].....	164
E.3	confidentiality protection strength.....	165
E.3.1	[CONF-SSM] Confidentiality protecting persistent storage for confidential data	165
E.3.1.1	General.....	165
E.3.1.2	[CONF-SSM-E-Basic] CONF.SSM.Basic confidentiality protecting secure storage mechanism.....	166
E.3.1.3	[CONF-SSM-E-Medium] CONF.SSM.Medium confidentiality protecting secure storage mechanism ..	166
E.3.1.4	[CONF-SSM-E-Enhanced] CONF.SSM.Enhanced confidentiality protecting secure storage mechanism	166
E.3.1.5	[CONF-SSM-E-Strong] CONF.SSM.Strong confidentiality protecting secure storage mechanism	166
E.3.2	Assessment for confidentiality protecting secure storage mechanism strength.....	166
E.3.2.1	General.....	166
E.3.2.2	Assessment criteria for [CONF-SSM-E-Basic]	167
E.3.2.3	Assessment criteria for [CONF-SSM-E-Medium].....	167
E.3.2.4	Assessment criteria for [CONF-SSM-E-Enhanced]	168
E.3.2.5	Assessment criteria for [CONF-SSM-E-Strong]	169
E.3.3	[CONF-COM] Communication of confidential data.....	170
E.3.3.1	General.....	170
E.3.3.2	[CONF-COM-E-Basic] CONF.COM.Basic confidentiality protecting communication mechanism	170
E.3.3.3	[CONF-COM-E-Medium] CONF.COM.Medium confidentiality protecting communication mechanism	170
E.3.3.4	[CONF-COM-E-Enhanced] CONF.COM.Enhanced confidentiality protecting communication mechanism	170
E.3.3.5	[CONF-COM-E-EndAuth] CONF.COM.Medium and CONF.COM.Enhanced confidentiality protecting communication mechanism endpoint authentication.....	171
E.3.3.6	[CONF-COM-E-Downgrade] CONF.COM.Medium and CONF.COM.Enhanced confidentiality protecting communication mechanism downgrade protection.....	171
E.3.4	Assessment for confidentiality protecting communication mechanism strength.....	171
E.3.4.1	General.....	171
E.3.4.2	Assessment criteria for [CONF-COM-E-Basic]	171
E.3.4.3	Assessment criteria for [CONF-COM-E-Medium]	172
E.3.4.4	Assessment criteria for [CONF-COM-E-Enhanced]	173
E.3.4.5	Assessment criteria for [CONF-COM-E-EndAuth].....	174
E.3.4.6	Assessment criteria for [CONF-COM-E-Downgrade]	175
Annex F (informative):	Guidance for the application of the present document	177
Annexes G to J:	Void.....	180

Annex K (normative):	Generic requirements and assessment criteria for the use of state of the art cryptography.....	181
K.1	Cryptography.....	181
K.1.1	Requirement	181
K.1.2	Assessment of product cryptographic configuration	182
K.1.2.0	General.....	182
K.1.2.1	Assessment of ACM-listed cryptographic mechanisms.....	182
K.1.2.1.1	Assessment objective	182
K.1.2.1.2	Assessment preparation.....	182
K.1.2.1.3	Assessment activities	182
K.1.2.1.4	Assessment evidence.....	183
K.1.2.1.5	Assessment verdict.....	183
K.1.2.2	Assessment of ACM-extended cryptographic mechanisms.....	183
K.1.2.2.1	Assessment objective	183
K.1.2.2.2	Assessment preparation.....	183
K.1.2.2.3	Assessment activities	183
K.1.2.2.4	Assessment evidence.....	184
K.1.2.2.5	Assessment verdict.....	184
K.1.2.3	Assessment of interoperability-based cryptographic mechanisms.....	184
K.1.2.3.1	Assessment objective	184
K.1.2.3.2	Assessment preparation.....	184
K.1.2.3.3	Assessment activities	184
K.1.2.3.4	Assessment evidence.....	185
K.1.2.3.5	Assessment verdict.....	185
K.2	Crypto agility.....	185
K.2.1	Requirement	185
K.2.2	Assessment of crypto-agility	186
K.2.2.1	Assessment objective	186
K.2.2.2	Assessment preparation	186
K.2.2.3	Assessment activities	187
K.2.2.4	Assessment evidence	187
K.2.2.5	Assessment verdict	187
K.3	ACM-extended cryptographic mechanisms	187
K.3.1	Requirement	187
K.3.2	List of ACM-extended cryptographic mechanisms.....	187
K.3.3	Assessment.....	188
K.4	Interoperability-based cryptographic mechanisms.....	188
K.4.1	Requirement	188
K.4.2	List of interoperability-based cryptographic mechanisms.....	188
K.4.3	Assessment.....	189
Annexes L to Q:	Void	190
Annex R (informative):	Guidance on RDPS	191
Annex S (informative):	Change history	192
History		193

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] to provide one voluntary means of conforming to the requirements of EU Regulation 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) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (CRA) [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 technical requirements and corresponding assessment criteria for personal wearable products that have a health monitoring purpose or that are intended for the use by and for children, related to cybersecurity. The products with digital elements in scope, thereafter "personal wearable":

- are specified within the "technical description" of the "category of product" number "19" by the Commission Implementing Regulation (EU) 2025/2392 of 28 November 2025 [i.2] as:
"Personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745(2) or (EU) 2017/746 of the European Parliament and of the Council do not apply, or personal wearable products that are intended for the use by and for children".
- 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 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] [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) No 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 TS 103 732-2 (V1.1.2): "CYBER; Consumer Mobile Device; Part 2: Biometric Authentication Protection Profile Module".

[i.7] ETSI EN 304 623 (V1.1.1): "Cyber Security (CYBER); CRA; Cybersecurity requirements for boot managers".

[i.8] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[i.9] IETF RFC 8613: "Object Security for Constrained RESTful Environments (OSCORE)".

[i.10] IETF RFC 9528: "Ephemeral Diffie-Hellman Over COSE (EDHOC)".

[i.11] IETF RFC 9147: "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

access control mechanism: personal wearable function that enforces an authorisation policy

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

actuator: device or component able to affect its physical environment as a result of command inputs

EXAMPLE: Electric motor, heater, etc.

adjacent communication: public communication limited to a logically adjacent topology or ingoing/outgoing communication to private networks

EXAMPLE: Intranet network (including VPN) or private mobile cellular network.

audio data: data asset that represents audio information processed by the personal wearable

audio input function: personal wearable function that converts audio signals into data

audio output function: personal wearable function that converts data into audio signals

authorisation policy: policy that describes the access rights of entities on personal wearable's data and functions

authentication mechanism: personal wearable function that verifies a claim of an entity about its identity

authorisation policy data: data asset that contains an authorisation policy

child: human entity under 14 years of age

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

configuration functionality: personal wearable function that allows to change the configuration of personal wearable's functions

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

connection function: personal wearable function that is used for testing or establishing communication capability via machine interface

EXAMPLE: ICMP, DHCP Discovery.

NOTE: Communication without user data and without authentication of the communication partner for the purpose of connection establishment.

controlled mobile operational environment: mobile operational environment where the user is expected to be constantly carrying the personal wearable

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 physical MP's operating system, hardware abstraction layer or APIs.

cryptographic mechanism: security-related procedure using cryptography

NOTE 1: The term "cryptographic mechanism" is used in this annex as an umbrella term covering the categories used in the ECCG Agreed Cryptographic Mechanisms (ACM) catalogue [reference], 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 the ECCG Agreed Cryptographic Mechanisms (ACM) catalogue [reference].

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 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: information in digital form

data asset: asset, that is data processed or stored by the personal wearable

default state: defined state where the configuration settings and configuration of the equipment is set to initial values

NOTE: A default state can include security updates, installed after the equipment being placed on the market.

device location data: data asset containing information on the geographical information of devices

factory reset function: personal wearable function that removes all user data and sets the MP in a factory default state, potentially keeping software updates

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

EXAMPLE: Private house or apartment.

function asset: asset, that is a function of the personal wearable

function trigger input: input to the RDPSs' or MP's functions provided by:

- human users, or
- sensor components of the MP or connected devices, or
- other devices or services

function output: output of RDPSs' or MP's functions that is:

- a modification or creation of personal wearables' data or functions, or
- information intended to inform human users, or
- information intended to inform or control devices or services, or
- information intended to control actuators, resulting in an action on the physical operational environment

function whose use can cause harm: function asset that is:

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

guardian: natural or legal entity with responsibility for the child

NOTE: This includes also parents.