



Cyber Security (CYBER); Cyber Resilience Act (CRA); Cybersecurity requirements for personal wearable products to be worn or placed on a human body that have a health monitoring purpose and for personal wearable products that are intended for the use by and for children

Exercising one of the **Principles of International Standardization – Openness** – and taking them to a different level, ETSI CYBER-EUSR has conducted open consultations on the vertical standards in support of the Cyber-Resilience Act, at a much earlier stage than it is usual in the standardization world. In this context, please keep in mind that the present document is an INTERIM draft, which expectably will be subject to substantial changes before their target publication date in the second semester of 2026.

ETSI CRA vertical standards v1.1.1 are being finalized and undergoing Public Enquiry via the National Standardization Organizations (NSO). Therefore, starting from 16 April 2026, ETSI CYBER-EUSR may only be able to address your comments in a future revision of the standard. **To enable ETSI CYBER-EUSR to address your comments before the first publication of the standards, you should cumulatively submit to your NSO any comments submitted here from 16 April 2026 onwards.** If you don't know how to do this, email us at cybersupport@etsi.org and we will guide you in the process.

Disclaimer: The INTERIM DRAFTS available for download in this page are provided for information and are for future development work within the ETSI Technical Committee CYBER EUSR Working Group (CYBER-EUSR) only. ETSI and its Members accept no liability for any further use/implementation of these specifications. Approved and published specifications and reports shall be obtained exclusively via the ETSI Documentation Service at <http://www.etsi.org/standards-search>

Commenting guidelines: Your comments to improve this early draft are very welcomed. To ensure the effectiveness of your contribution, please make sure to include the following elements in your comment:

1. Clear identification of the section of the draft your comment is referring to.
2. Objective proposal to delete content, add content or substitute content.
3. Concrete contribution (exact content you suggest including in the draft as an addition to, or in substitution of, existing content).
4. Brief rationale to justify the proposal (e.g. why the suggested content should be added an/or the existing content should be deleted or substituted).

Please note that comments without concrete contributions will be noted but not acted upon by ETSI CYBER-EUSR. We trust and value your expertise and therefore expect you to take this opportunity to proactively contribute to solving the issues you find while analysing this early draft.

Use of Artificial Intelligence (AI): Please do not use large language models to generate your comments. Inclusion of language generated by “AI” creates a potential for intellectual property conflicts and liability for ETSI, which is not acceptable.

How to comment: To comment or provide feedback on the present interim draft please send your comments to: cybersupport@etsi.org using the “[ETSI Commenting Format for Open Consultation.xlsx](https://docbox.etsi.org/CYBER/EUSR/Open)” available in <https://docbox.etsi.org/CYBER/EUSR/Open>

Feedback on your comments: The resolutions made in **Consensus** by ETSI CYBER-EUSR members, on each comment received through these Open Consultations will be published at the ETSI Open Area and ETSI Lab, assuring full **Transparency**.

Reference

DEN/CYBER-EUS-003

Keywords

CRA; Cybersecurity, wearables

0

ETSI

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

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

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

Important notice

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

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

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

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

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

Notice of disclaimer & limitation of liability

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

No recommendation as to products and services or vendors is made or should be implied.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

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

Copyright Notification

Reproduction is only permitted for the purpose of standardization work undertaken within ETSI.
The copyright and the foregoing restrictions extend to reproduction in all media.

© ETSI 2026.
All rights reserved.

1	Contents	
2	Intellectual Property Rights.....	7
3	Foreword.....	7
4	Modal verbs terminology	8
5	Executive summary	8
6	Introduction	8
7	1 Scope.....	9
8	2 References	9
9	2.1 Normative references.....	9
10	2.2 Informative references	9
11	3 Definition of terms, symbols and abbreviations.....	10
12	3.1 Terms	10
13	3.2 Symbols	13
14	3.3 Abbreviations.....	13
15	4 Product context.....	13
16	4.1 General.....	13
17	4.2 Intended purpose and reasonably foreseeable use	14
18	4.2.1 Wearable that have a health monitoring purpose	14
19	4.2.2 Wearable that are intended for the use by and for children.....	15
20	4.3 Product functions	15
21	4.3.1 Health monitoring functionalities (essential functionalities).....	15
22	4.3.2 Location-based functionalities (essential functionalities)	15
23	4.3.3 Notification functionalities (essential functionalities).....	16
24	4.3.4 Input commands from user or other connected devices (supporting functionalities).....	16
25	4.3.5 Data monitoring and storage (supporting functionalities).....	16
26	4.3.6 General functionalities (supporting functionalities).....	16
27	4.3.7 Summary of the wearable functions	17
28	4.3.8 Data assets.....	18
29	4.4 Product Architecture.....	18
30	4.4.1 Wearable that have a health monitoring purpose architecture.....	18
31	4.4.2 Wearable that are intended for the use by and for children architecture	20
32	4.5 Operational Environment.....	21
33	4.6 Interfaces.....	21
34	4.7 Users	22
35	4.7.1 End-Users.....	22
36	4.7.2 Manufacturers	22
37	4.8 Use cases profiles	22
38	4.8.1 Use case profile for basic impact essential functionalities	22
39	4.8.2 Use case profile for medium impact essential functionalities	22
40	4.8.3 Use case profile for high impact essential functionalities	23
41	4.9 Security Profiles.....	23
42	5 Requirements specifications.....	23
43	5.1 Product's technical requirements specifications.....	24
44	5.1.1 Known exploitable vulnerabilities.....	24
45	5.1.1.1 [NKEV] No known exploitable vulnerabilities	24
46	5.1.1.2 [NKEV-SUM] Secure software update mechanism	24
47	5.1.1.3 [NKEV-SUM-PROVIDE] Secure software update mechanism for core components	24
48	5.1.2 Default configuration	24
49	5.1.3 Authentication and access control mechanisms	25
50	5.1.3.1 [ACM-FH] Access control for functions whose use can cause harm	25
51	5.1.3.2 [AUM-FH] Authentication for functions whose use can cause harm.....	26
52	5.1.3.3 [AUTHZ-LP] Least privilege in authorization policies.....	27
53	5.1.3.4 [AUTHZ-R] Revocability of granted permissions	27

54	5.1.4	Integrity protection.....	27
55	5.1.4.1	[INT-SWPCK] Software package verification.....	27
56	5.1.4.2	[INT-COM] Communication of integrity relevant data.....	27
57	5.1.5	Confidentiality protection.....	28
58	5.1.5.1	[CONF-SSM] Confidentiality protecting persistent storage for confidential data.....	28
59	5.1.5.2	[CONF-COM] Communication of confidential data.....	28
60	5.1.6	Data minimization.....	29
61	5.1.6.1	[DMIN-DJST] Documented justification of processed data.....	29
62	5.1.7	Availability protection.....	29
63	5.1.7.1	[AVAI-TIME-RECO-POW] Restoration after loss of power.....	29
64	5.1.7.2	[AVAI-TIME-NETW] Local operation.....	29
65	5.1.7.3	[AVAI-TIME-RECO-NETW] Restoration after loss of network connection.....	29
66	5.1.7.4	[AVAI-TIME-OUTA-NOT] Notify non-availability.....	29
67	5.1.7.5	[AVAI-TIME-PREV-NOT] Notify upcoming limitation.....	29
68	5.1.7.6	[AVAI-TIME-PREV-PRIO] Network prioritization.....	29
69	5.1.7.7	[AVAI-TIME-RES-PRIO] Resource prioritization.....	30
70	5.1.7.8	[AVAI-TIME-IMP-AMP] Amplification control.....	30
71	5.1.7.9	[AVAI-TIME-DOS-RATE] Incoming rate limiting.....	30
72	5.1.7.10	[AVAI-UPD-SCHEDULE] Scheduling of updates.....	30
73	5.1.8	Impact minimization.....	30
74	5.1.9	Limit attack surface.....	30
75	5.1.9.1	[LAS-INVAL] Validation of external data input.....	30
76	5.1.9.2	[LAS-INSAN] Sanitization of external data input.....	30
77	5.1.9.3	[LAS-PHY-INF] Only necessary physical interfaces.....	31
78	5.1.9.4	[LAS-LOGIC-INF] Only necessary logical interfaces active by default.....	31
79	5.1.9.5	[LAS-APP] Only necessary apps by default.....	31
80	5.1.10	Logging and monitoring mechanisms.....	31
81	5.1.11	Deletion mechanisms.....	31
82	5.1.12	Other product's technical requirements specifications.....	31
83	5.2	Requirements specifications for vulnerability handling activities related to the product.....	31
84	6	Assessing for compliance with requirements.....	31
85	6.1	Assessing for compliance with product's technical requirements specifications.....	31
86	6.1.1	General.....	31
87	6.1.2	Known exploitable vulnerabilities.....	32
88	6.1.3	Default configuration.....	32
89	6.1.3.1	Assessment criteria for [SDC-FRM].....	32
90	6.1.4	Authentication and access control mechanisms.....	32
91	6.1.4.1	Assessment criteria for [ACM-FH].....	32
92	6.1.4.2	Assessment criteria for [AUM-FH].....	34
93	6.1.4.3	Assessment criteria for [AUTHZ-LP].....	35
94	6.1.4.4	Assessment criteria for [AUTHZ-R].....	35
95	6.1.5	Integrity protection.....	36
96	6.1.6	Confidentiality protection.....	36
97	6.1.7	Data minimization.....	36
98	6.1.7.1	Assessment criteria for [DMIN-DJST].....	36
99	6.1.8	Availability protection.....	38
100	6.1.8.1	Assessment criteria for [AVAI-TIME-RECO-POW].....	38
101	6.1.8.2	Assessment criteria for [AVAI-TIME-NETW].....	39
102	6.1.9	Impact minimization.....	40
103	6.1.10	Limit attack surface.....	40
104	6.1.11	Logging and monitoring mechanisms.....	41
105	6.1.12	Deletion mechanisms.....	41
106	6.1.13	Other product's technical requirements specifications.....	41
107	6.2	Assessment criteria for vulnerability handling activities related to the product.....	41
108	Annex A (informative): Relationship between the present document and the requirements of EU		
109	Regulation 2024/2847.....		42
110	Annex B (informative): Guidance for the application of the present document.....		48

111	Annex C (informative): Information on the methodology for the assessment of cybersecurity risks	
112	used to develop the present document	51
113	C.1 Guidance for determining impact classes.....	51
114	C.1.1 General.....	51
115	C.1.2 Confidential data.....	51
116	C.1.3 loss sensitive data	51
117	C.1.4 time sensitive data and time sensitive function.....	52
118	C.1.5 integrity relevant data and integrity relevant function	52
119	Annex D (normative): Relationship between specific data and functions assets covered by the	
120	present document to impact classes for generic asset categories.....	54
121	D.1 Identifier.....	54
122	D.2 Data assets	56
123	D.3 Function assets	57
124	D.3.1 Functions.....	57
125	D.3.2 Functions whose use can cause harm.....	58
126	Annex E (normative): Protection measures	59
127	E.1 Identifier.....	59
128	E.2 access control mechanism's strength.....	60
129	E.3 authentication mechanism strength	60
130	E.3.1 AUM-FH Authentication for functions whose use can cause harm.....	60
131	E.3.1.1 General	60
132	E.3.1.2 Authentication strength level basic	60
133	E.3.1.3 Authentication strength level medium.....	60
134	E.3.1.4 Authentication strength level enhanced.....	60
135	E.3.1.5 Authentication strength level strong.....	61
136	E.3.2 Assessment for authentication mechanism strength	61
137	E.3.2.1 Assessment criteria regarding the protection against limited presentation attacks.....	61
138	E.3.2.2 Assessment criteria regarding the protection against targeted presentation attacks	62
139	E.3.2.3 Assessment criteria regarding the protection against elaborate presentation attacks	62
140	E.3.2.4 Assessment criteria regarding the protection against limited brute force attacks.....	63
141	E.3.2.5 Assessment criteria regarding the protection against targeted brute force attacks	64
142	E.3.2.6 Assessment criteria regarding the protection against automated brute force attacks	64
143	E.3.2.7 Assessment criteria regarding the protection against presentation attacks	65
144	E.3.2.8 Assessment criteria regarding the protection against elaborate brute force attacks	66
145	E.3.2.9 Assessment criteria regarding the protection against automated security token spoofing attacks	66
146	E.3.2.10 Assessment criteria regarding the protection against targeted security token spoofing attacks	67
147	E.3.2.11 Assessment criteria regarding the protection against elaborate security token spoofing attacks	67
148	E.3.2.12 Assessment criteria regarding the protection against replay attacks	68
149	E.3.2.13 Assessment criteria regarding the protection against PitM attacks	69
150	E.4 confidentiality protection strength.....	70
151	E.4.1 CONF-SSM Confidentiality protecting persistent storage for confidential data	70
152	E.4.1.1 General	70
153	E.4.1.2 confidential persistent storage strength level basic	70
154	E.4.1.3 confidential persistent storage strength level medium	70
155	E.4.1.4 confidential persistent storage strength level enhanced	70
156	E.4.1.5 confidential persistent storage strength level strong.....	70
157	E.5 confidentiality protection strength.....	70
158	E.5.1 CONF-COM Communication of confidential data.....	70
159	E.5.1.1 General	70
160	E.5.1.2 communication of confidential data protection strength level basic	70
161	E.5.1.3 communication of confidential data protection strength level medium	71
162	E.5.1.4 communication of confidential data protection strength level enhanced.....	71
163	E.5.1.5 communication of confidential data protection strength level strong.....	71
164	E.6 integrity protection strength.....	71

165	E.6.1	INT-SWPCK Software package verification	71
166	E.6.1.1	General	71
167	E.6.1.2	software package integrity verification strength level basic	71
168	E.6.1.3	software package integrity verification strength level medium	72
169	E.6.1.4	software package integrity verification strength level enhanced	72
170	E.6.2	INT-COM Communication of integrity relevant data.....	72
171	E.6.2.1	General	72
172	E.6.2.2	communication of integrity relevant data protection strength level basic	72
173	E.6.2.3	communication of integrity relevant data protection strength level medium.....	72
174	E.6.2.4	communication of integrity relevant data protection strength level enhanced.....	72
175	E.6.2.5	communication of integrity relevant data protection strength level strong.....	73
176	Annex F (informative): Relationship between the present document and the covered/not covered		
177	cybersecurity risks		74
178	Annex G (informative):		77
179	Relationship between the present document and ETSI EN 303 645/ ETSI TS 103 701.....		77
180	Annex H (informative): Change history		78
181	History		79
182			
183			

184 Intellectual Property Rights

185 Essential patents

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

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

195 Trademarks

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

200 **DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its
 201 Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the
 202 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of
 203 the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

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

205 Foreword

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

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

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

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

221

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

222

223 Modal verbs terminology

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

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

228 Executive summary

229 "Executive summary" clause should be deleted if not necessary.

230 Introduction

231 "Introduction" clause should be deleted if not necessary.

232

233 1 Scope

234 The present document specifies activities, technical characteristics, cybersecurity requirements and corresponding
235 assessment criteria for personal wearable products to be worn or placed on a human body:

- 236 1) that have a health monitoring purpose; or
237 2) that are intended for the use by and for children

238 within the product context described in clause 4.

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

241 2 References

242 2.1 Normative references

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

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

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

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

- 251 [1] prEN 40000-1-3: "Cybersecurity requirements for products with digital elements - Vulnerability
252 Handling".

253 2.2 Informative references

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

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

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

- 261 [i.1] [Regulation \(EU\) 2024/2847](#) on horizontal cybersecurity requirements for products with digital
262 elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive
263 (EU) 2020/1828 (Cyber Resilience Act)

- 264 [i.2] [Commission Implementing Regulation \(EU\) 2025/2392](#) of 28 November 2025 on the technical
265 description of the categories of important and critical products with digital elements pursuant to
266 Regulation (EU) 2024/2847 of the European Parliament and of the Council.

- 267 [i.3] [Standardisation request M/606 - C\(2025\)618](#): "Commission Implementing decision of 3.2.2025 on
268 a standardisation request to the European Committee for Standardisation (CEN), the European
269 Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications
270 Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU)
271 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal
272 cybersecurity requirements for products with digital elements and amending Regulations (EU) No
273 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)".

274 [i.4] CEN/CLC JT013095:2026 (CEN/CLC prEN 40000-1-1): "Cybersecurity requirements for
275 products with digital elements – Vocabulary".

276 3 Definition of terms, symbols and abbreviations

277 3.1 Terms

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

280 **access control policy:** policy that describes the access rights of entities on wearable's data and functions

281 **access control mechanism:** wearable function that enforces an access control policy

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

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

285 EXAMPLE: electric motor, heater, etc.

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

288 EXAMPLE: intranet network (including VPN) or private mobile cellular network

289 **audio input data:** data asset that represents audio information captured by the wearable

290 **audio input function:** wearable function that converts audio signals into data

291 **audio output function:** wearable function that converts data into audio signals

292 **authorization policy:** policy that describes the access rights of entities on wearable's data and functions

293 **authentication mechanism:** wearable function that verifies an entity's claim

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

295 **child:** human entity under 14 years of age

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

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

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

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

302 EXAMPLE: ICMP, DHCP Discovery

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

305 **controlled mobile operational environment:** mobile operational environment where the user is expected to be
306 constantly carrying the wearable

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

309 EXAMPLE: A physical MP's operating system, hardware abstraction layer or APIs

- 310 **data:** information in digital form
- 311 **data asset:** asset, that is data processed or stored by the wearable
- 312 **device location data:** data asset containing information on the geographical information of devices
- 313 **factory reset function:** wearable function that removes all user data and sets the MP in a factory default state,
314 potentially keeping software updates
- 315 **fully controlled physical operational environment:** physical operational environment, where physical access is fully
316 controlled by the user or trusted persons
- 317 EXAMPLE: Private house or apartment.
- 318 **function asset:** asset, that is a function of the wearable
- 319 **function trigger input:** input to the RDPSs' or MP's functions provided by:
- 320 • human users, or
- 321 • sensor components of the MP or connected devices, or
- 322 • other devices or services
- 323 **function output:** output of RDPSs' or MP's functions that is:
- 324 • a modification or creation of wearables' data or functions, or
- 325 • information intended to inform human users, or
- 326 • information intended to inform or control devices or services, or
- 327 • information intended to control actuators, resulting in an action on the physical operational environment
- 328 **function whose use can cause harm:** function asset that is:
- 329 • a function whose use can impact the availability of other devices, services or networks,
- 330 • a function whose use can impact the safety or privacy of human user
- 331 • a function who can communicate confidential data,
- 332 • a function who can communicate integrity relevant data,
- 333 • a function who can modify integrity relevant data, or
- 334 • a function who can modify integrity relevant functions
- 335 **guardian:** natural or legal entity with responsibility for the child
- 336 NOTE: This includes also parents.
- 337 **health data:** data asset that indicates information about physiological functions, health condition or physical fitness of
338 humans
- 339 **human interface:** interface that is intended to be used by human
- 340 **integrity relevant data:** data asset, whose tampering can have a negative impact
- 341 **integrity relevant function:** function asset, whose tampering can have a negative impact
- 342 **interface:** shared boundary across which the wearable exchanges information
- 343 **local communication:** ingoing/outgoing communication which requires physical access to a communication partner's
344 interface or proximity of the communication partner to the wearable
- 345 EXAMPLE: WLAN interface, Bluetooth Interface or wired interfaces such as Ethernet or USB.

- 346 **location data:** data containing geographical information
- 347 **logging mechanism:** wearable function that logs events
- 348 **logical interface:** interface that does not exist in hardware and can only be used by using another device or a physical
349 interface of a wearable
- 350 **logical operational environment:** operational environment describing the accessibility via logical interfaces
- 351 **loss sensitive data:** data asset, whose permanent loss has a negative impact
- 352 **machine interface:** interface that is intended to be used for machine-to-machine communication
- 353 **main product:** wearable without the remote data processing solution
- 354 **mobile operational environment:** physical operational environment, where the geographical location is changing
355 during operation and not confined to a specific area
- 356 NOTE: Physical operational environment of smartphones and wearables
- 357 **network status data:** data asset that describes MPs' or RDPSs' network connections status
- 358 **notification mechanism:** wearable function that notifies entities on certain events
- 359 **partially controlled physical operational environment:** physical operational environment, that is not a fully
360 controlled physical operational environment and either under the control of a limited set of persons or located in an area
361 where untrusted physical access is suspicious
- 362 EXAMPLE: Shared area in a house with different apartments or private property where public access is not
363 intended.
- 364 **personal calendar data:** data asset that represents information on a personal calendar
- 365 **personal contact data:** data asset that represents personal contact information of entities
- 366 **personal notes data:** data asset that represents personal information other than calendar data or contact data
- 367 **physical communication:** communication that requires manipulation of the communication partner's hardware or the
368 hardware the communication partner runs on
- 369 EXAMPLE:
- 370 **physical interface:** interface that is part of the hardware of a wearable
- 371 **physical operational environment:** operational environment describing the physical accessibility
- 372 **physical security function:** wearable function which provides function output as reaction to function trigger input
373 related to residential physical security
- 374
- 375 **public communication:** ingoing/outgoing communication to public networks
- 376 EXAMPLE: internet network or mobile cellular network
- 377 **public data:** data from publicly accessible sources
- 378 **public data asset:** data asset derived from public data
- 379 **sensor:** device or component able to measure characteristics of its physical environment, generating data input
380 representative of its physical environment
- 381 EXAMPLE: Blood pressure sensor, heart rate monitor, accelerometer, etc.
- 382 **software update mechanism:** wearable function that allows to change the wearable's software
- 383 **strictly local communication:** ingoing/outgoing communication which requires physical presence at a communication
384 partner's interface

385 EXAMPLE: NFC or other short-range communication

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

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

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

391 EXAMPLE: Areas intended for public access

392 **user data:** data provided by a user

393 **video input data:** data asset that represents video information captured by the wearable

394 **video input function:** wearable function that converts video signals into data

395 **video output function:** wearable function that converts data into video signals

396 **wearable:** product with digital element

397 NOTE: In the contest of the present document the wearable is the defined as in [i.1] and [i.2]

398 3.2 Symbols

399 Void.

400 3.3 Abbreviations

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

402	GPS	Global Positioning System
403	MP	Main Product
404	RDPS	Remote Data Processing Solution

405

406

407 4 Product context

408 4.1 General

409 Two kinds of products are considered in the present document: wearable that have a health monitoring purpose and
410 wearable that are intended for the use by and for children. As per CRA [i.1], hardware and software products may fall in
411 this category, but most products include a combination of hardware (including sensors and some processing
412 capabilities) and hosted software.

413 Non-exhaustive examples of wearable that have a health monitoring purpose are:

414 • smart watches;

415 • fitness bands;

416 • smart glasses

417 • heart rate monitor,

418 • smart socks;

419 • headbands;

420 • biomechanical shoe insoles;

421 • skin patches

422 Wearable that are intended for the use by and for children can be divided in two categories depending to the age of the
423 child. There is a clear separation between the wearables for babies under 2-year-old, for which the monitoring is much
424 more extensive but without the need of the baby to manage the device, and the preadolescent children where GPS
425 tracking and Parental Control are key functionalities.

426 Non-exhaustive examples of wearable that are intended for the use by and for preadolescent children are:

427 • smartwatches with GPS tracking and parental control

428 Non-exhaustive examples of wearable that are intended for the use by and for babies under 2-year-old are:

429 • baby monitoring system including:

430 - baby smart socks

431 - sensor bracelet for breathing monitoring

432 - Smart wearable breast pumps

433 - Smart pacifiers - with temperature check-ups and GPS tracker

434 4.2 Intended purpose and reasonably foreseeable use

435 4.2.1 Wearable that have a health monitoring purpose

436 The main intended uses of this category of wearables are:

- 437 1) the health monitoring which means the continuous collection, analysis and visualization of physiological and
438 health-related data (e.g. heart rate data, blood oxygen levels, stress data or other vital signs) using sensors
439 included in the wearable;
- 440 2) the activity tracking which means collecting and analysing (automatically or on demand) data like the number
441 of steps done, distance gone, exertion, intensity and burned calories during activities like walking, jogging,
442 bicycling, swimming, dancing; etc.

443 Several use cases can be derived from the two main intended uses listed above:

- 444 1) productivity use cases which involve monitoring of user's activity. Wearable devices track activity such a step,
445 walking patterns, walking speed, posture, identifying periods of rest and fatigue. Using this information,
446 wearable can raise awareness about the lifestyle patterns, provide scheduled or situation-based notifications
447 (e.g. work breaks, rests, or walks).
- 448 2) wellness use cases which include monitoring of stress levels, providing medication reminders, monitoring
449 sleep patterns and heart rate patterns, identifying abnormal health events and long-term health trends,
450 supporting better rest and recovery of the human body, supporting hygiene routines (e.g. hand hygiene), and
451 offer safety features (e.g. fall detection and alerts for elderly users).
- 452 3) fitness and sports use cases which involve monitoring of relevant physiological data to get insights into fitness
453 condition, fitness performance to optimize training and sports tactics.
- 454 4) safety use cases which involve supporting personal safety and environmental awareness. Wearable devices
455 provide alerts (e.g. fall detection, SOS), notifications (e.g. user fatigue) and share user's location (e.g. to other
456 team members).
- 457 5) interactive experiences use cases which involve integrated sensory experiences and real-time feedback (e.g.
458 virtual reality, art installations) and educational programs that enhance learning by increasing motivation and
459 engagement. Wearable devices capture physiological data such as body movements, hand movements
460 electroencephalography (EEG), eye tracking, heart rate.

4.2.2 Wearable that are intended for the use by and for children

The main intended uses of this category of wearables are:

- 1) the health monitoring which means the continuous collection, analysis and visualization of physiological and health-related data (e.g. heart rate data, blood oxygen levels, stress data or other vital signs) using sensors included in the wearable.
- 2) The location tracking to monitor the child position.
- 3) Parental control to allow children parents to control the child activities on the wearables.

4.3 Product functions

This clause lists the essential functionalities associated with the wearable's intended use.

4.3.1 Health monitoring functionalities (essential functionalities)

It includes the physiological data acquisition using sensors, physiological data signal processing, analysis and visualization. Examples of sensors include light source and photodetector, accelerometers, gyroscopes, temperature sensor, skin response sensor, pulse oximeter sensor (SP0₂), skin temperature, skin conductance, non-invasive surface electrodes, microphones, piezoelectric sensors, smart glasses.

Examples of health monitoring functionalities include:

- the health monitoring which means the continuous collection, analysis and visualization of physiological and health-related data (e.g. heart rate data, blood oxygen levels, stress data or other vital signs) using sensors included in the wearable.
- heart-rate, electrocardiography and heart variability monitoring.
- blood oxygen saturation.
- stress monitoring.
- fatigue detection.
- respiratory rate.
- step counting, posture detection, fall detection.
- sleep monitoring.
- skin temperature, skin conductance.
- muscle activity.
- electroencephalography.
- vibrations detection, capturing heart and breathing sounds.

NOTE: The list above is provided as guidance only; it is not complete or future-proof.

4.3.2 Location-based functionalities (essential functionalities)

It includes activities regarding to the user's position. They may rely on radio technologies such as indoor radio (e.g. Bluetooth[®], Wi-Fi[®]), outdoor radio (e.g. cellular, GPS), or light-based technologies (e.g. LED).

Examples of main location -based functionalities include:

- navigation which guides movement from one place to another;
- tracking which monitors user location;

- 497 • localization which determines the precise location;
- 498 • geofencing which creates virtual boundaries.
- 499 • the location tracking to monitor the children position.

500 NOTE: The list above is provided as guidance only; it is not complete or future-proof.

501 4.3.3 Notification functionalities (essential functionalities)

502 It includes real-time alerts, messages, reports and reminders. They may rely on displays/LEDs, haptic actuators and
503 speakers or a companion mobile application.

504 Examples of notification functionalities include:

- 505 • reminders and recommendations: activity (break, relaxation), hydration, medication, bedtime;
- 506 • detections: stress, heart-rate, fall, heart-rate zone, fitness condition, trends;
- 507 • alarms: environmental hazard, fall, SOS, timers.

508 NOTE: The list above is provided as guidance only; it is not complete or future-proof.

509 4.3.4 Input commands from user or other connected devices (supporting 510 functionalities)

511 It includes interactions with the wearable using technologies such as touch screen, buttons, voice, gestures, biometrics
512 and other sensors, and commands from other connected devices.

513 4.3.5 Data monitoring and storage (supporting functionalities)

514 It includes monitoring of physiological data, environment data, behavioural data, name, health condition, trends and
515 storage of personal data such as age, weight, height, gender, and relies on wearable's memories.

516 4.3.6 General functionalities (supporting functionalities)

517 General functionalities are essential to allow the wearable to provide the main uses cases and the essential
518 functionalities described in the previous clauses. General functionalities describe core, non-specialized functionalities of
519 a wearable that support everyday interaction, usability, and system integration. These include functions such as device
520 setup, account management, synchronization with smartphones or cloud services, battery status monitoring, user
521 customization and updatability. The general functionalities are listed below:

- 522 • software update: The wearable checks for and installs firmware or software updates to ensure security, bug
523 fixes and feature enhancements;
- 524 • factory reset mechanism: reset the wearable to the factory default state;
- 525 • registration: user have to register and log into a service account (e.g. to activate the wearable, sync data, or
526 access cloud-based features/services);
- 527 • device pairing and setup: during initial setup, the wearable pairs with a connected device (e.g. smartphone) and
528 walks the user through configuration steps like account login, preferences, and permissions;
- 529 • configuration: set, modify, configure and personalize the wearable's settings;
- 530 • deactivation: deactivate on the wearable certain services or the collection of certain data;
- 531 • data synchronization and backup: synchronize data with companion mobile application and/or cloud service
532 and backup data on the cloud application;
- 533 • security functionalities: the functionalities that protect the data assets.

534 NOTE: The list above is provided as guidance only; it is not complete or future-proof.

535 4.3.7 Summary of the wearable functions

536 The present document addresses the following wearable essential functionalities:

- 537 • health monitoring functionalities
- 538 • activity monitoring functionalities
- 539 • positioning functionalities
- 540 • location sharing functionalities
- 541 • emergency location functionalities
- 542 • location sharing functionalities (for children use)
- 543 • parental control functionalities
- 544 • audio input functionalities
- 545 • video input functionalities
- 546 • notification functionalities
- 547 • audio output functionalities
- 548 • video output functionalities
- 549 • functionalities which can communicate wearable data assets

550 The present document addresses the following wearable supporting functionalities:

- 551 • logging mechanism
- 552 • input sanitization mechanism
- 553 • input validation mechanism
- 554 • configuration functionalities
- 555 • software update mechanism
- 556 • access control mechanism
- 557 • authentication mechanism
- 558 • factory reset function
- 559 • integrity protecting communication mechanism
- 560 • confidentiality protecting communication mechanism
- 561 • integrity protecting secure storage mechanism
- 562 • confidentiality protecting secure storage mechanism
- 563 • deletion mechanism
- 564 • onboarding mechanism
- 565 • software package verification mechanism
- 566 • bootloader functionalities

567 • time service or functionalities

568 • real-time service or clock

569 4.3.8 Data assets

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

571 • health data;

572 • activity data;

573 • input data from sensors;

574 • location data, including device location data;

575 • location data (for children use), including device location data;

576 • geofencing (for children use)

577 • audio input data;

578 • video input data;

579 • audio output data;

580 • video output data;

581 • audio input data (for children use);

582 • video input data (for children use);

583 • audio output data (for children use);

584 • video output data (for children use);

585 • network status data;

586 • access control policy data;

587 • social interactive data

588 • social interactive data (for children use);

589 • confidential data;

590 • personal calendar data;

591 • personal contact data;

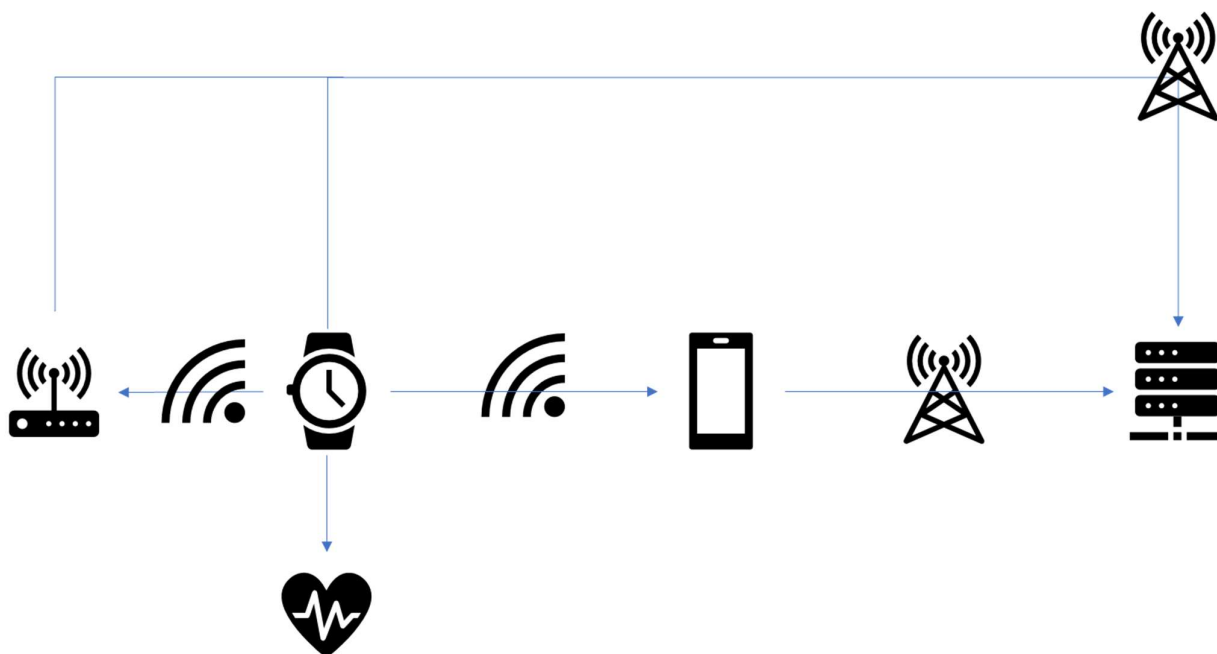
592 • personal notes data.

593 4.4 Product Architecture

594 This clause describes the two architectures for the wearables in the scope of the present document.

595 4.4.1 Wearable that have a health monitoring purpose architecture

596 The architecture of the health monitoring wearable is shown in Figure 1.



597

598

Figure 1: Health monitoring wearable architecture

599

600

- 1) The wearable device hosts several sensors, and through internal interfaces between the main processor and the sensors, it collects data about health and user activities.

601

602

603

604

605

606

- 2) The wearable device may be connected to a mobile application running typically on a mobile phone. The local radio link between them can be any type, typically Bluetooth® or Wi-Fi. Through this link the wearable device transfers to the mobile application the health data collected, the notifications, alerts, reminders and any other data needed to support its functionalities. If the wearable is a standalone device, or if it has the possibility to be directly connected to a cloud service (e.g. through an internet connection over Wi-Fi or cellular) it might not have an associated mobile application.

607

NOTE 1: The mobile application may be considered a remote data processing solution.

608

609

610

611

612

613

- 3) The mobile application associated to the wearable device may be connected to a remote service hosted in the cloud. The radio link may be Wi-Fi or mobile connection. Through this link the mobile application may transfer to the cloud service some processed data, activity report, health report and a backup of all the mobile application data, e.g. in order to be able to move the application on another mobile device if the user decide to change it. The remote service to which the mobile application is connected may also provide software updates for the wearable device that will be delivered through the link described in point 2.

614

NOTE 2: Under the CRA [i.1], the cloud service constitutes a remote data processing solution.

615

616

617

618

619

- 4) The wearable device in some cases is directly connected to a server hosting its cloud application (e.g. through a Wi-Fi or mobile connection). The radio link is most likely Wi-Fi or mobile connection. Through this link the wearable device transfers to the cloud application processed data, activity report, health report and a backup of all the wearable device data in order to be able to move them on another wearable device if the user decide to change it. The server to which the wearable device is connected can be also provide software updates.

620

NOTE 3: The cloud service may be considered a remote data processing solution.

621

622

- 5) The wearable device in some cases may be connected via a local connection to a gateway that perform then the remote connection to the cloud service.

623

Therefore, the architecture of wearable device consists of the following architectural components:

624

- The main product (hardware and software)

625

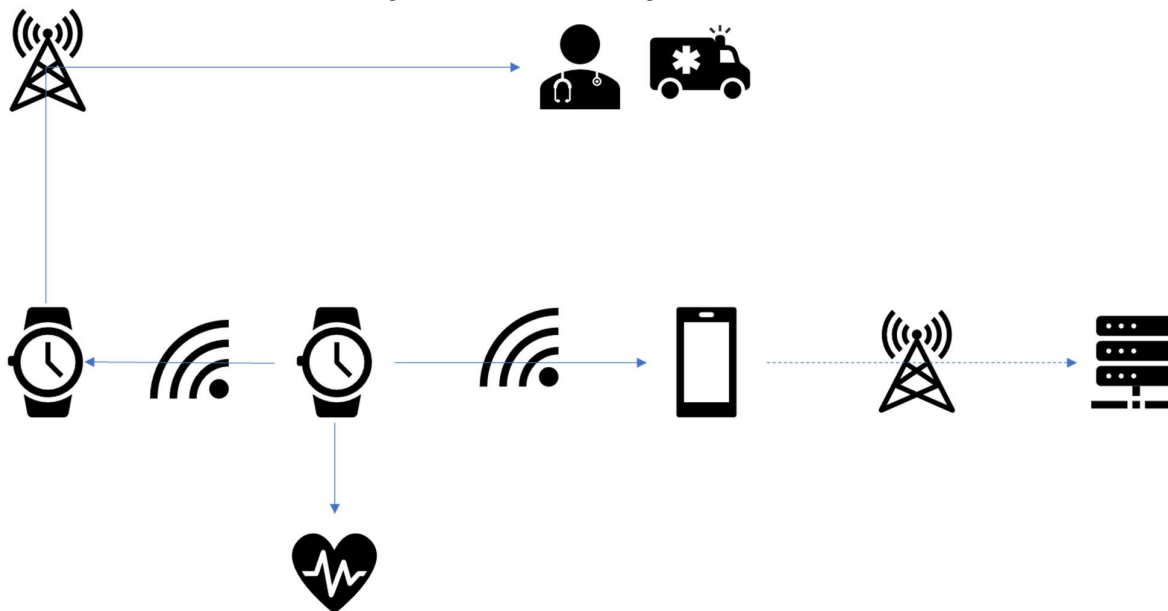
- The mobile application acting as remote data processing service (optional)

- 626 • The cloud service acting as remote data processing service (optional)
- 627 • The gateway (optional)

628 4.4.2 Wearable that are intended for the use by and for children

629 architecture

630 The architecture of the health monitoring wearable is shown in Figure 2.



631

632

Figure 2: Health monitoring wearable architecture

- 633 1) The wearable device hosts several sensors, and through internal interfaces between the main processor and the sensors, it collects data about health and user activities.
- 634
- 635 2) The wearable device may be connected to a mobile application on a mobile phone. The radio link can be any
- 636 type, typically Bluetooth® or Wi-Fi. Through this link the wearable device transfers to the mobile application
- 637 the health data collected, the notifications, alerting, reminders and any other data needed to allow its
- 638 functionalities. If the wearable is a standalone device or if it has the possibility to be directly connected to a
- 639 remote cloud service (e.g. through an internet connection over Wi-Fi or cellular) it might not have an
- 640 associated mobile application.

641 NOTE 1: Under the CRA [i.1], the mobile application may be considered a remote data processing solution.

- 642 3) The mobile application associated to the wearable device may be connected to a remote cloud service. The
- 643 radio link may be Wi-Fi or cellular. Through this link the mobile application transfers to the cloud application
- 644 processed data, activity report, health report and a backup of all the mobile application data, e.g. in order to be
- 645 able to move the application on another mobile device if the user decide to change it. The remote service to
- 646 which the mobile application is connected may also provide software updates for the wearable device that will
- 647 be delivered through the link described in point 2.

648 NOTE 2: Under the CRA [i.1], the cloud application constitutes a remote data processing solution.

- 649 4) The wearable device in some cases is locally connected to another wearable device, usually controlled by the
- 650 children's parents, which may perform a connection with remote emergency services infrastructure where
- 651 needed (e.g. through an internet connection over Wi-Fi or cellular). Through this link the wearable device may
- 652 transfer emergency requests and trigger the intervention of emergency staff, where necessary.

653 NOTE 3: Under the CRA [i.1], the emergency services infrastructure constitutes a remote data processing solution.

654 Therefore, the architecture of wearable device consists of the following architectural components:

- 655 1) The main product (hardware and software)
- 656 2) The mobile application acting as remote data processing service (optional)
- 657 3) The cloud application acting as remote data processing service (optional)
- 658 4) The emergency services infrastructure acting as remote data processing solution (optional)

659 4.5 Operational Environment

660 Common wearable devices placements include, but are not limited to, the wrist, finger, head, chest, clothing, shoes or
661 belts. Wearables may operate continuously (24/7) or only be activated during specific activities (e.g. exercise). Their
662 autonomy depends on battery life and recharge cycles and charging is handled via wired connectors, magnetic docks, or
663 wireless power.

664 The physical environment of the wearable devices may include all typical consumer electronic physical environments,
665 including homes, offices, wellness centres, but also outdoor spaces such as rural areas, city streets, sport stadiums.
666 Wearable devices typically follow a user-centric trust model, assuming that the user will not attempt to compromise the
667 device (e.g. alter the data) and the data is trustworthy before it leaves the device, however this may not hold in all user
668 contexts, for example a user may have incentives to manipulate his/her location. Moreover, the presence of radio
669 interfaces in wearables (e.g. NFC, BLE, Wi-Fi) may expose them to external threats including the risk of receiving
670 malicious software and unauthorized commands, and even physical risks such as battery overheating.

671 For the physical operational environment, the following environments are addressed for the MPs.

- 672 • fully controlled physical operational environment - POE.FullyControlled
- 673 • partially controlled physical operational environment - POE.PartiallyControlled
- 674 • mobile operational environment - POE.Mobile
- 675 • controlled mobile operational environment - POE.MobileControlled

676 For the physical operational environment, the following environments are addressed for the mobile application RDPS:

- 677 • fully controlled physical operational environment - POE.FullyControlled
- 678 • partially controlled physical operational environment - POE.PartiallyControlled
- 679 • mobile operational environment - POE.Mobile

680 For the physical operation environment, the following environments are addressed for cloud service (RDPSs):

- 681 • fully controlled physical operational environment - POE.FullyControlled.

682 Logical environments include the connected systems around the main product that shape how it operates in its
683 environment. The trusted boundary is affected by potential third party software that runs on the wearable, data links to
684 the outside world using radio interfaces, and user permissions and access control.

685 For the logical operation environment, the following digital communication types are addressed for any architectural
686 component of the wearable.

- 687 • public communication - COM.Public
- 688 • adjacent communication - COM.Adjacent
- 689 • local communication - COM.Local
- 690 • strict local communication – COM.StrictLocal

691 4.6 Interfaces

692 The present document addresses the following interfaces of the wearable:

- 693 • human interface - IF.Human
- 694 • machine interface - IF.Machine
- 695 • logical interface - IF.Logical
- 696 • physical interface - IF.Physical

697 4.7 Users

698 4.7.1 End-Users

699 They acquire the wearable and connect it to the wearable manufacturer ecosystem using state-of-the-art security
700 methods. They may have access to the information via the wearable device display, via the mobile application or
701 another connected device. They may control who has access to their data and which third-party applications are
702 installed on the wearable device. In the case of children, supervisors (such as parents or guardians) maintain control
703 over these settings.

704 4.7.2 Manufacturers

705 Manufacturers deliver the product to market which may be coming together with a manufacturer mobile application and
706 Remote Data Platform services. Guidelines are provided to the end-user for setting-up the wearable and connecting the
707 wearable to the mobile phone or generally to the internet using state-of-the art security methods. Manufacturers are
708 pushing software updates to the wearable device and keep the software updated. Depending on the privacy agreements,
709 terms of service and regulatory compliance the manufacturers may have access to the end-user data or not.

710 4.8 Use cases profiles

711 The present document addresses all use cases that can be constructed by the elements of clause 4.

712 In order to classify use cases and to define security profiles the following use case profiles are defined. Those
713 definitions make use of impact classes of essential functionalities. The essential functionalities covered by the present
714 document are provided in clause 4.3.7, their impact classes are provided in annex D.

715 4.8.1 Use case profile for basic impact essential functionalities

716 The use case profile for basic impact essential functionalities bundles all use cases addressed by the present document
717 where the maximum (IMP.FH, IMP.AVAI.TIME) of a wearable's essential functionality falls under IMP.Low.

718 Example of such use cases profile are:

- 719 • wearables measuring activity data not related to health data such as, for example, smart socks, biomechanical
720 shoe.

721 NOTE: most of the wearable in this use case profile may not have any display and or audio/speaker system therefore
722 no audio/video input/output.

723 4.8.2 Use case profile for medium impact essential functionalities

724 The use case profile for basic impact essential functionalities bundles all use cases addressed by the present document
725 where the maximum (IMP.FH, IMP.AVAI.TIME) of a wearale's essential functionality falls under IMP.Medium.

726 Example of such use cases profile are:

- 727 • wearables measuring health data and providing location services even for emergency call such as, for example,
728 smart watches, smart glasses, heart rate monitor band, etc ...

729 4.8.3 Use case profile for high impact essential functionalities

730 The use case profile for high impact essential functionalities bundles all use cases addressed by the present document
731 where the maximum (IMP.FH, IMP.AVAI.TIME) of a wearable's essential functionality falls under IMP.High.

732 Example use cases:

- 733 • wearables providing positioning for emergency services or wearables used by children supporting parental
734 control and geofencing functionalities.

735 4.9 Security Profiles

736 Based on the use case profiles defined in clause 4.8 the following security profiles with assigned requirements in table [1](#)
737 are defined:

- 738 • security profile for basic impact functions
- 739 • security profile for medium impact functions
- 740 • security profile for high impact functions

741 **Table 1: Security profiles with corresponding requirements**

Requirement	Security profile for		
	Low impact functions	Medium impact functions	High impact functions
[NKEV]	X	X	X
[NKEV-SUM]	X	X	X
[NKEV-SUM-PROVIDE]	X	X	X
[NKEV-SUM-AUTO]	X	X	X
[NKEV-SUM-NOTIF]	X	X	X
[SDC-AUM-FH]	X	X	X
[SDC-SUM-AUTO]	X	X	X
[SDC-UPD-NOTIF]	X	X	X
[SDC-FRM]	X	X	X
[ACM-FH]	X	X	X
[AUM-FH]	X	X	X
[AUTHZ-LP]	X	X	X
[AUTHZ-R]	X	X	X
[INT-SWPCK]	X	X	X
[INT-COM]	X	X	X
[CONF-SSM]	X	X	X
[CONF-COM]	X	X	X
[DMIN-DJST]	X	X	X
[AVAI-TIME-RECO-POW]	X	X	X
[AVAI-TIME-NETW]	X	X	X
[AVAI-TIME-RECO-NETW]	X	X	X
[AVAI-TIME-OUTA-NOT]		X	X
[AVAI-TIME-PREV-NOT]			X
[AVAI-TIME-PREV-PRIO]		X	X
[AVAI-TIME-RES-PRIO]		X	X
[AVAI-TIME-IMP-AMP]			
[AVAI-TIME-DOS-RATE]			
[AVAI-SUM-SCHEDULE]		X	X
[LAS-INVAL]	X	X	X
[LAS-INSAN]	X	X	X
[LAS-PHY-INF]	X	X	X
[LAS-LOGIC-INF]	X	X	X
[LAS-APP]	X	X	X

742

743 5 Requirements specifications

744 5.1 Product's technical requirements specifications

745 5.1.1 Known exploitable vulnerabilities

746 5.1.1.1 [NKEV] No known exploitable vulnerabilities

747 In accordance with [1] the wearable shall be tested prior to making available on the market to ensure that there are no
748 insufficiently mitigated known exploitable vulnerabilities.

749 NOTE 1: The known exploitable vulnerabilities that occur after making the wearable available on the market are
750 subject to the vulnerability handling in [1].

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

753 5.1.1.2 [NKEV-SUM] Secure software update mechanism

754 The wearable shall support software update mechanisms, that allow to update every part of the wearable's software,
755 except for parts of the wearable's software, that are immutable due to technical reasons.

756

757 EXAMPLE: An application distribution platform installed on a mobile device provides updates for mobile
758 applications acting as RDPS. In some cases, where the application to be updated is part of the
759 wearable's core software, the core software update mechanism provides also the application
760 updates.

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

762 5.1.1.3 [NKEV-SUM-PROVIDE] Secure software update mechanism for core 763 components

764 All architectural components of the wearable that include core software shall provide software update mechanisms, that
765 allow to update every part of the architectural components' software, except for parts of the architectural components'
766 software, that are immutable due to security.

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

768 5.1.1.4 [NKEV-UPD-AUTO] Automated security updates

769 The wearable shall support the automated update of its software.

770 5.1.1.5 [NKEV-UPD-NOTIF] Update notifications

771 The wearable shall support the automated notification of its users, when updates of its software are available.

772 5.1.2 Default configuration

773 5.1.2.1 [SDC-AUM-FH] Default configuration of authentication for functions whose 774 use can cause harm

775 The wearable shall, by default, be configured to use authentication mechanisms that meet:

- 776 • the authentication mechanisms strengths specified in clause E.3.1; and
- 777 • the minimal authentication mechanisms' strength determined by table 3;

778 except for connection functions.

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

780 5.1.2.2 [SDC-UPD-AUTO] Default configuration of automated security updates

781 The wearable shall, by default, be configured to use automated software update mechanisms for its software.

782 NOTE: The support of automated security updates is addressed in [NKEV-UPD-AUTO].

783 NOTE: The user can decide to turn off the automated security update mechanism and manually perform the
784 update when is more suitable for him. For example, the user does not want to update the wearable during
785 a sport session where health and activity data are monitored or when the software update can interfere
786 with parental control functionalities.

787

788 5.1.2.3 [SDC-UPD-NOTIF] Default configuration of update notifications

789 The wearable shall by default be configured to receive automated notification and alert its users, when updates of the
790 wearable's software are available.

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

792

793 5.1.2.4 [SDC-FRM] Factory reset to restore the default state

794 The wearable shall provide a factory reset mechanism that allows a user to restore the default state, including the
795 deletion of all user data, installed applications, and configurations deviating from the default state, except deviations
796 due to security.797 NOTE 1: It is also possible that the factory reset will delete the installed security updates if these are installed
798 automatically or on request when the device is commissioned again.799 NOTE 2: Annex II 8. d) of the CRA [i.1] contains legal obligations on how users of the wearable are informed
800 about secure decommissioning.

801 5.1.3 Authentication and access control mechanisms

802 5.1.3.1 [ACM-FH] Access control for functions whose use can cause harm

803 The wearable shall use access control mechanisms to control entities' use of functions whose use can cause harm, where
804 the applicability of this requirement is determined by table 2 except for connection functions.

805

Table 2: Assignment for access control mechanisms

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

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

806

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

- 809 • factory reset function
- 810 • functions configured by parental control function

811 **5.1.3.2 [AUM-FH] Authentication for functions whose use can cause harm**

812 The wearable shall support authentication mechanisms, to authenticate entities using functions whose use can cause
 813 harm before generating function output, where

- 814 • the authentication mechanisms strengths are specified in clause E..1; and
- 815 • the minimal required authentication strength is determined by table 3,

816 except for connection functions.

817

Table 3: Assignment for authentication mechanisms strengths

			impact class for function whose use can cause harm		
			IMP.FH.Basic	IMP.FH.Medium	IMP.FH.High
Attack Surface determined by COM, IF and POE of RDPS or MP that receives function trigger input	COM.StrictLocal via IF.Any	POE.FullyControlled	N/A	N/A	AUTH.Basic[1]
		POE.PartiallyControlled	N/A	AUTH.Basic[1]	AUTH.Medium[1]
		POE.Mobile	AUTH.Basic[1]	AUTH.Medium[1]	AUTH.Enhanced[1]
		POE.Controlled.Mobile	N/A	AUTH.Basic[1]	AUTH.Medium[1]
	COM.Local via IF.HumanPhysical	POE.FullyControlled	N/A	AUTH.Basic	AUTH.Medium
		POE.PartiallyControlled	AUTH.Basic	AUTH.Medium	AUTH.Enhanced
		POE.Mobile	AUTH.Basic	AUTH.Medium	AUTH.Enhanced
		POE.Controlled.Mobile	N/A	AUTH.Basic[1]	AUTH.Medium[1]
	COM.Local via a non-IF.HumanPhysical	POE.Any	AUTH.Medium	AUTH.Medium	AUTH.Enhanced
	COM.Adjacent via IF.Any		AUTH.Medium	AUTH.Medium	AUTH.Enhanced
COM.Public via IF.Any		AUTH.Medium	AUTH.Enhanced	AUTH.Enhanced	

818

819 For protection measures that are labelled with [1] it is not required that the wearable uses authentication mechanisms for
 820 its following functions:

- 821 • factory reset function
- 822 • functions configured by parental control function

823

824 5.1.3.3 [AUTHZ-LP] Least privilege in authorization policies

825 The wearable shall use an authorization policy that only grants permissions that are necessary for the intended purpose.

826 EXAMPLE: A wearable with just one consumer grants that consumer all permissions.

827 5.1.3.4 [AUTHZ-R] Revocability of granted permissions

828 The wearable shall support the revocation of any permission granted by an authorized entity.

829 EXAMPLE: An administrative consumer can revoke permissions granted to another consumer.

830 5.1.4 Integrity protection

831 5.1.4.1 [INT-SWPCK] Software package verification

832 The wearable shall use software package verification mechanisms to verify the integrity and authenticity of software
833 packages prior to installation where the software package verification mechanism's strength levels are specified in
834 clause E.6.1 and where the minimal software package verification mechanism's strength is determined by table 4.

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

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

		Highest IMP.INT of the SHPSF's integrity relevant functions		
		IMP.INT.Low	IMP.INT.Medium	IMP.INT.High
Attack Surface determined by the COM of RDPS or MP over which the software package is received	COM.Local	INT.SW.VER.Basic	INT.SW.VER.Basic	INT.SW.VER.Basic
	COM.Adjacent or COM.Public	INT.SW.VER.Medium	INT.SW.VER.Medium	INT.SW.VER.Enhanced

838

839

840 5.1.4.2 [INT-COM] Communication of integrity relevant data

841 The wearable shall use integrity protecting communication mechanisms to protect the integrity of communicated
842 integrity relevant data, where the corresponding integrity protection measures strengths are specified in clause E.6.2 and
843 the minimal required integrity protection measures' strength are determined by table 4.

844 **Table 5: Assignment of protection mechanisms strength level for the integrity protection of outgoing**
845 **data and for the integrity verification of incoming data**

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

846

847

848 **5.1.5 Confidentiality protection**849 **5.1.5.1 [CONF-SSM] Confidentiality protecting persistent storage for confidential**
850 **data**

851 The wearable shall use confidentiality protecting secure storage mechanisms for persistently stored confidential data,
852 where the mechanisms' strength are specified in clause E.4.1 and the minimal required mechanisms' strength are
853 determined by table 6.

854 NOTE: the requirement applies only to wearable's storage means; external storage means such as memory card
855 are out of the scope.

856 **Table 6: Assignment for confidentiality protecting secure storage mechanisms**

		Confidentiality impact class for persistently stored confidential data		
		IMP.CONF.Low	IMP.CONF.Medium	IMP.CONF.High
Attack Surface determined by POE of RDPS or MP that persistently stores confidential data	POE.FullyControlled	N/A	N/A	N/A
	POE.PartiallyControlled	N/A	CONF.SSM.Basic[1]	CONF.SSM.Medium
	POE.Mobile	CONF.SSM.Basic[1]	CONF.SSM.Normal	CONF.SSM.Enhanced
	POE.MobileControlled	N/A	CONF.SSM.Basic[1]	CONF.SSM.Medium

857

858 For protection measures labelled with [1], it is not required that the wearable uses confidentiality protecting persistent
859 storage for confidential data:

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

861

862 **5.1.5.2 [CONF-COM] Communication of confidential data**

863 The wearable shall use confidentiality protecting communication mechanisms to protect the confidentiality of
864 communicated confidential data, where the corresponding confidentiality protection measures strengths are specified in
865 clause E.5.1 and the minimal required confidentiality protection measures' strength are determined by table 7.

866 **Table 7: Assignment of protection mechanisms strength level for the confidentiality of**
867 **communicated data**

			confidential data impact class		
			IMP.CONF.Low	IMP.CONF.Medium	IMP.CONF.High
	COM.StrictLocal via IF.Human	POE.Any	N/A	N/A	CONF.COM.Basic
Attack Surface determined by COM, IF and POE of RDPS or MP that communicates confidential data	COM.Local via IF.Machine or IF.Human	POE.FullyControlled	N/A	N/A	CONF.COM.Medium
		POE.PartiallyControlled	N/A	CONF.COM.Basic	CONF.COM.Medium
		POE.Mobile	CONF.COM.Basic	CONF.COM.Medium	CONF.COM.Enhanced
		POE.MobileControlled	N/A	CONF.COM.Basic	CONF.COM.Medium
	COM.Adjacent via IF.Any	POE.Any	CONF.COM.Medium	CONF.COM.Enhanced	CONF.COM.Enhanced
	COM.Public via IF.Any		CONF.COM.Medium	CONF.COM.Enhanced	CONF.COM.Enhanced

868

869

870 5.1.6 Data minimization

871 5.1.6.1 [DMIN-DJST] Documented justification of processed data

872 The wearable shall only process confidential data according to its intended purpose.

873 5.1.7 Availability protection

874 5.1.7.1 [AVAI-TIME-RECO-POW] Restoration after loss of power

875 The MP shall use a mechanism to resume connectivity and functionality in the case of a loss of power as soon as the
876 power supply is restored.

877 5.1.7.2 [AVAI-TIME-NETW] Local operation

878 Where no network connectivity is necessary for a time sensitive function to operate, the wearable shall ensure the
879 operability of this function in the case of a loss of network access.

880 5.1.7.3 [AVAI-TIME-RECO-NETW] Restoration after loss of network connection

881 The wearable shall use a mechanism to reconnect cleanly after a loss of network connection.

882 EXAMPLE: A wearable loses connection to the local network as the network is temporarily unavailable. After
883 recognizing the restored network, the wearable reconnects after a randomized delay to reconnect
884 cleanly.

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

887 5.1.7.4 [AVAI-TIME-OUTA-NOT] Notify non-availability

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

891 EXAMPLE 1: A cloud RDPS recognizes a non-availability of its MP and sends a notification to the user.

892 5.1.7.5 [AVAI-TIME-PREV-NOT] Notify upcoming limitation

893 Where at least one time sensitive function with IMP.AVAI.TIME.High is provided by the wearable, the wearable shall
894 use a mechanism to notify the user before it restrains the use of power when the wearable recognises low power
895 condition.

896 EXAMPLE: A battery powered wearable recognizes low battery and sends a notification to the user.

897 5.1.7.6 [AVAI-TIME-PREV-PRIO] Network prioritization

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

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

903 5.1.7.7 [AVAI-TIME-RES-PRIO] Resource prioritization

904 Where at least one time sensitive function with IMP.AVAI.TIME.Medium or higher is provided by the wearable and
905 the wearable is intended to be powered by battery, the wearable shall use a mechanism to prioritize the use of power in
906 the case of a low power condition:

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

909

910 5.1.7.8 [AVAI-TIME-IMP-AMP] Amplification control

911 TBD

912 5.1.7.9 [AVAI-TIME-DOS-RATE] Incoming rate limiting

913 TBD

914 5.1.7.10 [AVAI-UPD-SCHEDULE] Scheduling of updates

915 Where at least one time sensitive function with IMP.AVAI.TIME.Medium or higher is provided by the ewearable, the
916 wearable shall support the scheduling of the application of updates that can impact the availability of these functions
917 with IMP.AVAI.TIME.Medium or higher.

918 5.1.8 Impact minimization

919 TBD

920 5.1.9 Limit attack surface

921 5.1.9.1 [LAS-INVAL] Validation of external data input

922 The wearable shall use input validation mechanisms for all external data input received via:

- 923 • local communication,
- 924 • adjacent communication and
- 925 • public communication.

926 EXAMPLE 1: If external data input via a specific interface is expected to be an email address, the wearable
927 rejects external data input that has not the format of an email address.

928 EXAMPLE 2: PIN pad, touch screen, web interface for user login and user product management are local
929 communication examples.

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

934 5.1.9.2 [LAS-INSAN] Sanitization of external data input

935 The wearable shall use input sanitization mechanisms at the application layer before using external data input where the
936 validation of external data input cannot prevent potential incidents triggered by the external data input.

937 EXAMPLE: If external data input is amongst others intended to be stored via a database service, escape
938 characters and other database service specific commands are removed from the external data input,
939 before it is processed by the database service.

940 5.1.9.3 [LAS-PHY-INF] Only necessary physical interfaces

941 A hardware MP shall only provide physical interfaces, that are necessary for the wearable's intended purpose.

942 5.1.9.4 [LAS-LOGIC-INF] Only necessary logical interfaces active by default

943 The wearable shall by default only use logical interfaces, that are necessary for its intended purpose.

944 5.1.9.5 [LAS-APP] Only necessary apps by default

945 The wearable shall by default only use application softwares, that are necessary for its intended purpose.

946 5.1.10 Logging and monitoring mechanisms

947 TBD

948 5.1.11 Deletion mechanisms

949 TBD

950 5.1.12 Other product's technical requirements specifications

951 **This subclause is intended to address cybersecurity risks that are identified but not covered by the ECRs of CRA**
952 **ANNEX I Part I (2).**

953 TBD

954 5.2 Requirements specifications for vulnerability handling
955 activities related to the product

956 The requirements specified in **prEN 40000-1-3 [1]** shall be fulfilled for the wearable.

957 6 Assessing for compliance with requirements

958 6.1 Assessing for compliance with product's technical
959 requirements specifications

960 6.1.1 General

961 In order to assess the compliance with the requirements listed in clause [5.1](#) of the present document, the assessment
962 procedures described in clause [6.1](#) are to be followed. When performing assessments, the distribution of security
963 functions (see clause [4.5](#)) are to be considered, including whether the product provides security functions itself,
964 demands them from other products with digital elements within its context, or supplies them to other products with
965 digital elements.

966 If there are already existing evidences (e.g. provided by manufacturers of components that are integrated in the
967 wearable) that:

- 968
- are covering the same assessment activities as described in clause [6.1](#), and
 - are valid for the moment of the assessment to be performed under clause [6.1](#),
- 969

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

971 6.1.2 Known exploitable vulnerabilities

972 6.1.2.1 Assessment criteria for [NKEV-MKAV]

973 6.1.3 Default configuration

974 6.1.3.1 Assessment criteria for [SDC-FRM]

975 **Assessment objective:**

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

978 **Assessment preparation:**

- 979 • Documentation on how the factory reset mechanism can be accessed.
- 980 • The wearable shall be set up and some configuration changes shall be created and persistently stored.
- 981 • Where the wearable supports the storage of user data, some user data shall be created and persistently stored
982 on the wearable.
- 983 • Where the wearable supports the installation of applications, some common application for the wearable shall
984 be installed.

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

986 **Assessment activities:**

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

991 **Assignment of verdict:**

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

994 The verdict FAIL shall be assigned otherwise.

995 **Supporting Evidence:**

- 996 • Description of the performed test
- 997 • All test records of the performed test.

998 6.1.4 Authentication and access control mechanisms

999 6.1.4.1 Assessment criteria for [ACM-FH]

1000 **Assessment objective:**

1001 The assessment covers:

- 1002 • a conceptual assessment of ACM-FH
- 1003 • a functional completeness assessment on the wearable capabilities that are addressed by ACM-FH
- 1004 • a functional sufficiency assessment of each access control mechanism used by the wearable to fulfil ACM-FH

1005 based on the default configuration required by clause 5.1.2.

1006 **Assessment preparation:**

1007 The following documentation for the wearable shall be complete:

- 1008 • a list of wearable's functions whose use can cause harm
- 1009 • for each function, whose use can cause harm:
 - 1010 - its impact class impact class for function, whose use can cause harm
 - 1011 - the physical operational environment of the architectural component that performs the function
 - 1012 - for each of the function's trigger input possibilities:
 - 1013 ▪ the interface and communication type
 - 1014 ▪ a list of corresponding access control mechanisms including their default authorization policy.

1015 The following test setups shall be prepared:

- 1016 • a test setup for identifying functions, their trigger input possibilities and corresponding access control
1017 mechanisms based on a sample wearable in default configuration,
- 1018 • for each access control mechanism, a test setup that allows privilege escalation attacks from authenticated
1019 entities and unauthorized access attempts of unauthenticated entities.

1020 **Assessment activities:**

- 1021 • The wearable's conformity to ACM-FH shall be validated based on the documentation.
- 1022 • The correctness and completeness of the documentation shall be verified by:
 - 1023 - an inspection of the wearable for functions and related access control mechanisms that are accessible via
1024 physical human interfaces
 - 1025 - a scan of the wearable for functions and related access control mechanisms that are accessible via logical
1026 interfaces.
- 1027 • For each access control mechanism, its correct implementation shall be verified based on attempts to violate
1028 the authorization policy by:
 - 1029 - privilege escalation of authenticated entities based on the default authorization policy
 - 1030 - unauthorized usage of function, whose use can cause harm by unauthenticated entities based on the
1031 default authorization policy.

1032 **Assignment of verdict:**

1033 The verdict PASS shall be assigned if:

- 1034 • the documentation indicates the wearable's conformity to ACM-FH; and
- 1035 • the verification of the correctness and completeness of the documentation was successful; and
- 1036 • the verification of the correct implementation of each access control mechanism was successful.

1037 The verdict FAIL shall be assigned otherwise.

1038 **Supporting Evidence:**

- 1039 • records of the validation of the documentation
- 1040 • descriptions of the performed tests and records of performed tests to verify the correctness and completeness
1041 of the documentation

- 1042 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each
1043 access control mechanism

1044 6.1.4.2 Assessment criteria for [AUM-FH]

1045 **Assessment objective:**

1046 The assessment covers:

- 1047 • a conceptual assessment of AUM-FH
- 1048 • a functional completeness assessment on the wearable capabilities that are addressed by AUM-FH
- 1049 • a functional sufficiency assessment of each authentication mechanism used by the wearable to fulfil AUM-FH
- 1050 based on the default configuration required by clause [5.1.2](#).

1051 **Assessment preparation:**

1052 The following documentation for the wearable shall be complete:

- 1053 • a list of wearable's functions whose use can cause harm
- 1054 • for each function, whose use can cause harm:
- 1055 - its impact class impact class for function, whose use can cause harm
- 1056 - the physical operational environment of the architectural component that performs the function
- 1057 - for each of the function's trigger input possibilities:
- 1058 ▪ the interface and communication type
- 1059 ▪ a list of corresponding authentication mechanisms including:
- 1060 • the authentication mechanisms' strength
- 1061 • the type of authentication factors.

1062 The following test setups shall be prepared:

- 1063 • a test setup for identifying functions, their trigger input possibilities and corresponding authentication
1064 mechanisms based on a sample wearable in default configuration,
- 1065 • for each authentication mechanism, a test setup defined by the test cases provided in clause [E.3](#) according to
1066 the needs determined by its strength and the type of its authentication factors.

1067 **Assessment activities:**

- 1068 • The wearable's conformity to ACM-FH shall be validated based on the documentation.
- 1069 • The correctness and completeness of the documentation shall be verified by:
- 1070 - an inspection of the wearable for functions and related authentication mechanisms that are accessible via
1071 physical human interfaces
- 1072 - a scan of the wearable for functions and related authentication mechanisms that are accessible via logical
1073 interfaces.
- 1074 • For each authentication mechanism, its correct implementation shall be verified based on the test cases
1075 provided in clause [E.3](#) according to the needs determined by its strength and the type of its authentication
1076 factors.

1077 **Assignment of verdict:**

1078 The verdict PASS shall be assigned if:

- 1079 • the documentation indicates the wearable's conformity to ACM-FH; and
- 1080 • the verification of the correctness and completeness of the documentation was successful; and
- 1081 • the verification of the correct implementation of each authentication mechanism was successful.

1082 The verdict FAIL shall be assigned otherwise.

1083 **Supporting Evidence:**

- 1084 • records of the validation of the documentation
- 1085 • descriptions of the performed tests and records of performed tests to verify the correctness and completeness
- 1086 of the documentation
- 1087 • descriptions of the performed tests and records of performed tests to verify the correct implementation of each
- 1088 authentication mechanism.

1089 **6.1.4.3 Assessment criteria for [AUTHZ-LP]**

1090 **Assessment objective:**

1091 The assessment covers:

- 1092 • a conceptual assessment of AUTHZ-LP.

1093 based on the default configuration required by clause [5.1.2](#).

1094 **Assessment preparation:**

1095 The following documentation for the wearable shall be complete:

- 1096 • a description of the authorization policies in default configuration including:
- 1097 - a list of granted permissions for entities on function, whose use can cause harm and
- 1098 - for each granted permission, a justification that it is necessary for the intended purpose.

1099 **Assessment activities:**

- 1100 • The wearable's conformity to {requirement_authz:AUTHZ-LP} shall be validated based on the
- 1101 documentation.

1102 **Assignment of verdict:**

1103 The verdict PASS shall be assigned if:

- 1104 • the documentation indicates the wearable's conformity to AUTHZ-LP.

1105 The verdict FAIL shall be assigned otherwise.

1106 **Supporting Evidence:**

- 1107 • records of the validation of the documentation.

1108 **6.1.4.4 Assessment criteria for [AUTHZ-R]**

1109 **Assessment objective:**

1110 The assessment covers:

- 1111 • a functional sufficiency assessment to ensure the wearable supports revocation of any granted permissions.

1112 **Assessment preparation:**

1113 The following documentation for the wearable shall be complete:

- 1114 • a list of mechanisms to grant permissions for entities on function, whose use can cause harm.

1115 The following test setups shall be prepared:

- 1116 • for each mechanism to grant permissions, a test setup for granting and revoking permissions for entities on
1117 function, whose use can cause harm.

1118 **Assessment activities:**

- 1119 • For each mechanism to grant permissions, the revocability of grantable permissions shall be verified by:
- 1120 - granting permissions to an entity,
- 1121 - revoking the permissions, and
- 1122 - attempting use permissions after revocation.

1123 **Assignment of verdict:**

1124 The verdict PASS shall be assigned if:

- 1125 • for each mechanism to grant permissions, access is denied after revocation.

1126 The verdict FAIL shall be assigned otherwise.

1127 **Supporting Evidence:**

- 1128 • descriptions of the performed tests and records of performed tests to verify the correct implementation of
1129 AUTHZ-R.

1130 **6.1.5 Integrity protection**

1131 **6.1.6 Confidentiality protection**

1132 **6.1.7 Data minimization**

1133 **6.1.7.1 Assessment criteria for [DMIN-DJST]**

1134 **Assessment objective:**

1135 The assessment covers:

- 1136 • a conceptual assessment of Documented justification of processed data
- 1137 • a functional sufficiency assessment of each mechanism and/or configuration used by the wearable to fulfil
1138 Documented justification of processed data
- 1139 • a functional completeness assessment on the wearable capabilities that are addressed by Documented
1140 justification of processed data.

1141 **Assessment preparation:**

1142 The following documentation for the wearable shall be complete:

- 1143 • a list of all documented data sources and destinations to which processed data is transmitted or made
1144 accessible (if applicable), processed by the wearable in its default configuration;
- 1145 • a list of all data assets processed by the wearable whose impact class for confidential wearable data is
1146 IMP.CONF.Low or higher;
- 1147 • for each documented confidential data asset, the associated rationale for its necessity explaining why its
1148 processing is necessary for the intended purpose of the wearable;

- 1149 • a description of the mechanisms and/or configurations used to ensure data minimization (e.g. code modules for
1150 data filtering, configuration settings that limit data intake, architectural diagrams showing data flows, or
1151 policies that prevent unnecessary processing).

1152 NOTE: The documentation of sources and destinations may be combined where a data flow is bidirectional or
1153 where source and destination are the same entity.

1154 The following shall be prepared:

- 1155 • a methodology capable of detecting and listing all data sources actually processed by an wearable in its default
1156 configuration and, where applicable, the destinations (set up communication partners) to which data is
1157 transmitted or made accessible (e.g. network traffic analysis, log inspection, dynamic analysis tools,
1158 source-code review where available, interface enumeration, etc.);
- 1159 • test setups to evaluate the data minimization mechanisms and/or configurations, including attempts to trigger
1160 or configure the wearable to process additional data beyond the documented and justified items (e.g. via
1161 configuration changes, input simulations, or interface probing), based on the described mechanisms and/or
1162 configurations.

1163 **Assessment activities:**

- 1164 • the correctness and completeness of the documentation shall be verified by:
- 1165 - using the prepared methodology, identify and list all data sources (and destinations, if applicable) that are
1166 actually processed by the sample wearable in its default configuration;
- 1167 - comparing the identified data sources/destinations with the documented list;
- 1168 - for every confidential data item that is documented, verifying that a clear and plausible rationale is
1169 provided showing that its processing is necessary for the intended purpose and reasonably foreseeable
1170 use;
- 1171 - verifying that no confidential data item is processed for which no documentation or no sufficient
1172 rationale exists;
- 1173 - reviewing the described data minimization mechanisms and/or configurations for conceptual sufficiency
1174 (e.g. ensure they align with best practices for limiting data to necessities, such as least-privilege data
1175 access or runtime checks); and
- 1176 - performing functional tests on the mechanisms and/or configurations using the prepared test setups to
1177 confirm they prevent or restrict processing of undocumented or unjustified data (e.g. attempt to enable
1178 optional data collection features and verify if they are disabled by default or require explicit justification;
1179 simulate inputs that could lead to extra data processing and check if they are filtered or ignored).

1180 **Assignment of verdict:**

1181 The verdict PASS shall be assigned if:

- 1182 • all actually processed data sources/destinations are documented;
- 1183 • every documented data item has a sufficient rationale demonstrating necessity for the intended purpose and
1184 reasonably foreseeable use;
- 1185 • no undocumented or unjustified confidential data processing is observed;
- 1186 • the described mechanisms and/or configurations are conceptually sufficient to enforce data minimization; and
- 1187 • functional tests confirm that the mechanisms and/or configurations only process necessary data.

1188 Otherwise, the verdict FAIL shall be assigned.

1189 **Supporting Evidence:**

- 1190 • descriptions of the performed tests and documentation of associated test records to verify the correctness and
1191 completeness of the documentation

- 1192 • descriptions of the performed tests and documentation of associated test records that verify the correct
1193 implementation of each data minimization mechanism and/or configuration

1194 6.1.8 Availability protection

1195 6.1.8.1 Assessment criteria for [AVAI-TIME-RECO-POW]

1196 **Assessment objective:**

1197 The assessment covers:

- 1198 • a functional sufficiency assessment of the recovery function interaction with each power supply used by the
1199 wearable's MP to fulfil AVAI-TIME-RECO-POW

1200 based on the default configuration required by clause [5.1.2](#).

1201 **Assessment preparation:**

1202 The following documentation for the wearable shall be complete:

- 1203 • a list of all power supplies used by the wearable's MP
- 1204 - for each power supply: a description whether a power supply can power the MP alone
- 1205 • a list of all functionalities of the wearable that need communication involving the MP
- 1206 - for each of these functionalities:
- 1207 ▪ a list of interfaces of the wearable, where the connection status of the necessary communication
1208 channels can be read; OR
- 1209 ▪ parameters of the necessary communication channel of the MP in order to externally observe if the
1210 connection is active
- 1211 - a list of interfaces of the wearable, where the operational status of the MP can be read
- 1212 ▪ description how the operational status can be implied from the interface readings.

1213 The following test setups shall be prepared:

- 1214 • the wearable is set up in default configuration
- 1215 • a test setup to:
- 1216 - safely disconnect or disable and reconnect or enable the power supplies of the wearable's MP
- 1217 - enable access to at least one interfaces of the wearable, where the operational status of the wearable can
1218 be read
- 1219 - enable access to at least one interfaces of the wearable, where the connection status the necessary
1220 communication channels status of the MP can be read
- 1221 - if the connection status for all necessary communication channels of the MP cannot be read from the
1222 wearable:
- 1223 ▪ monitor whether all necessary communication channels of the MP are active.

1224 **Assessment activities:**

1225 The following activities shall be performed:

- 1226 • for every possible order in which the MPs power supplies can be disconnected or disabled:
- 1227 - disconnect or disable the all power supplies of the MP
- 1228 - wait at least 30s

- 1229 - reconnect or enable the power supplies
- 1230 - monitor the operational status of the wearable
- 1231 - monitor the connection status for all necessary communication channels of the MP
- 1232 - record the order in which the power supplies are disconnect or disable and reconnect or enable
- 1233 - record the time relative to the reconnection or enabling of the last power supply, after which the wearable
1234 indicates, that it is operational and all necessary communication channels are established; OR
- 1235 - record the time relative to the reconnection or enabling of the last power supply, after which every
1236 necessary communication channels of the MP was active at least once, and there is no indication that the
1237 wearable has not resumed operation.

1238 **Assignment of verdict:**

1239 The verdict PASS shall be assigned if:

- 1240 • the wearable signals resume of operations and establishment of all necessary communication channels within
1241 one hour after the reconnection or enabling of the last power supply; OR
- 1242 • all necessary communication channels of the MP were active at least once, and there is no indication that the
1243 wearable has not resumed operation within one hour
- 1244 • The verdict FAIL shall be assigned otherwise.

1245 **Supporting Evidence:**

- 1246 • descriptions of the performed tests and records of performed tests.

1247 **6.1.8.2 Assessment criteria for [AVAI-TIME-NETW]**

1248 **Assessment objective:**

1249 The assessment covers:

- 1250 • a conceptual assessment of AVAI-TIME-NETW
- 1251 • a functional completeness assessment on the wearable capabilities that are addressed by AVAI-TIME-NETW
- 1252 • a functional sufficiency assessment of each time sensitive function without the need of network connectivity to
1253 operate used by the wearable to fulfil AVAI-TIME-NETW

1254 based on the default configuration required by clause [5.1.2](#).

1255 **Assessment preparation:**

1256 The following documentation for the wearable shall be complete:

- 1257 • a list of all time sensitive function of the wearable
- 1258 - for each time sensitive function:
- 1259 - description of the functionalities realised or supported by this function
- 1260 - list of interfaces necessary for the operation of this function
- 1261 ▪ for each interface:
- 1262 ▪ communication types of the interface
- 1263 • a list of interfaces of the wearable, where the status of the MPs time sensitive function can be read
- 1264 - description how the status can be implied from the interface readings.

1265 The following test setups shall be prepared:

- 1266
- the wearable is set up in default configuration
- 1267
- a test setup to:
 - 1268 - disconnect or disable the public communication of the wearable's MP
 - 1269 - disconnect or disable the adjacent communication of the wearable's MP
 - 1270 - enable access to at least one interfaces of the wearable, where the status of the wearable's time sensitive
 - 1271 function can be read

1272 **Assessment activities:**

1273 The following activities shall be performed:

- 1274
- verify the correctness and completeness of the documentation
- 1275
- repeat the following steps for communication types public communication, adjacent communication and both,
1276 depending on the communication type needed by the functions to be tested:
 - 1277 - disconnect or disable the corresponding communication type of the wearable's MP
 - 1278 - wait at least 30s
 - 1279 - for each time sensitive function which does not need any interface with the corresponding
1280 communication type for its operation
 - 1281 ▪ check whether the function is in operable status
 - 1282 ▪ record the status of the function and the disconnected or disabled communication type
 - 1283 - reconnect or enable the corresponding communication type.

1284 **Assignment of verdict:**

1285 The verdict PASS shall be assigned if:

- 1286
- no indication, that the documentation is incorrect or incomplete, are found
- 1287
- all checked time sensitive functions are in operable state

1288 The verdict FAIL shall be assigned otherwise.

1289 **Supporting Evidence:**

- 1290
- descriptions of the performed tests and records of performed tests.

1291 **6.1.9 Impact minimization**

1292 **6.1.10 Limit attack surface**

1293

1294 6.1.11 Logging and monitoring mechanisms

1295 6.1.12 Deletion mechanisms

1296 6.1.13 Other product's technical requirements specifications

1297 6.2 Assessment criteria for vulnerability handling activities
1298 related to the product

1299 The assessment criteria specified in CEN/CLC JT013090:2026 (CEN/CLC prEN 40000-1-3) [1] shall be met for the
1300 SHGPVA based on the corresponding specified input and output.

1301 **Annex A (informative):**
1302 **Relationship between the present document and the**
1303 **requirements of EU Regulation 2024/2847**

1304 The present document has been prepared under the Commission's Standardisation request M/606 - C(2025)618 [i.3] to
1305 provide one voluntary means of conforming to the requirements of Regulation (EU) No 2024/2847 of the European
1306 Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital
1307 elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber
1308 Resilience Act).

1309 Once the present document is cited in the Official Journal of the European Union under that Regulation, compliance
1310 with the normative clauses of the present document given in table A.1 confers, within the limits of the scope of the
1311 present document, a presumption of conformity with the corresponding requirements of that Regulation and associated
1312 EFTA regulations.

1313
1314

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

Harmonised Standard ETSI EN 304 634					
Requirement				Requirement Conditionality	
No	Description	Requirements of Regulation	Clause(s) of the present document	U/C	Condition
1	The design, development, and production of products with digital elements ensures an appropriate level of cybersecurity based on the risks.	Annex I, Part I, (1)	[[ACM-FH] 5.1.3.1 [AUM-FH] 5.1.3.2 [AUTHZ-LP] 5.1.3.3 [AUTHZ-R] 5.1.3.4 [AVAI-TIME-RECO-POW] 5.1.7.1 [AVAI-TIME-NETW] 5.1.7.2 [AVAI-TIME-RECO-NETW] 5.1.7.3 [AVAI-TIME-OUTA-NOT] 5.1.7.4 [AVAI-TIME-PREV-NOT] 5.1.7.5 [AVAI-TIME-NET-PRIO] 5.1.7.6 [AVAI-TIME-RES-PRIO] 5.1.7.7 [AVAI-TIME-IMP-AMP] 5.1.7.8 [AVAI-TIME-DOS-RATE] 5.1.7.9 [AVAI-SUM-SCHEDULE] 5.1.7.10 [CONF-SSM] 5.1.5.1 [CONF-COM] 5.1.5.2 [DMIN-DJST] 5.1.6.1 [INT-SWPCK] 5.1.4.1 [INT-COM] 5.1.4.2 [LAS-INVAL] 5.1.9.1 [LAS-INSAN] 5.1.9.2 [LAS-PHY-INF] 5.1.9.3 [LAS-LOGIC-INF] 5.1.9.4 [LAS-APP] 5.1.9.5 [NKEV] 5.1.1.1 [NKEV-SUM] 5.1.1.2 [NKEV-SUM-PROVIDE] 5.1.1.3 [NKEV-SUM-AUTO] 5.1.1.4 [NKEV-SUM-NOTIF] 5.1.1.5 [SDC-AUM-FH] 5.1.2.1 [SDC-SUM-AUTO] 5.1.2.2 [SDC-SUM-NOTIF] 5.1.2.3 [SDC-FRM] 5.1.2.4	U	
2	Products with digital elements are made available on the market without known exploitable vulnerabilities.	Annex I, Part I, (2)(a)	[[NKEV] 5.1.1.1]	U	
3	Products with digital elements are made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state.	Annex I, Part I, (2)(b)	[[LAS-LOGIC-INF] 5.1.9.4 [LAS-APP] 5.1.9.5 [SDC-AUM-FH] 5.1.2.1 [SDC-SUM-AUTO] 5.1.2.2 [SDC-SUM-NOTIF] 5.1.2.3 [SDC-FRM] 5.1.2.4]	U	

Harmonised Standard ETSI EN 304 634					
Requirement				Requirement Conditionality	
No	Description	Requirements of Regulation	Clause(s) of the present document	U/C	Condition
4	Products with digital elements ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them.	Annex I, Part I, (2)(c)	[[NKEV-SUM] 5.1.1.2 [NKEV-SUM-PROVIDE] 5.1.1.3 [NKEV-SUM-AUTO] 5.1.1.4 [NKEV-SUM-NOTIF] 5.1.1.5 [SDC-SUM-AUTO] 5.1.2.2 [SDC-SUM-NOTIF] 5.1.2.3]	U	
5	Products with digital elements ensure protection from Unauthorized access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible Unauthorized access.	Annex I, Part I, (2)(d)	[[ACM-FH] 5.1.3.1 [AUM-FH] 5.1.3.2 [AUTHZ-LP] 5.1.3.3 [AUTHZ-R] 5.1.3.4 [SDC-AUM-FH] 5.1.2.1]	U	
6	Products with digital elements protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means.	Annex I, Part I, (2)(e)	[[CONF-SSM] 5.1.5.1 [CONF-COM] 5.1.5.2]	U	
7	Products with digital elements protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorized by the user, and report on corruptions.	Annex I, Part I, (2)(f)	[[INT-SWPCK] 5.1.4.1 [INT-COM] 5.1.4.2]	U	
8	Products with digital elements process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimization).	Annex I, Part I, (2)(g)	[[DMIN-DJST] 5.1.6.1]	U	

Harmonised Standard ETSI EN 304 634					
Requirement				Requirement Conditionality	
No	Description	Requirements of Regulation	Clause(s) of the present document	U/C	Condition
9	Products with digital elements protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks.	Annex I, Part I, (2)(h)	[[AVAI-TIME-RECO-POW] 5.1.7.1 [AVAI-TIME-NETW] 5.1.7.2 [AVAI-TIME-RECO-NETW] 5.1.7.3 [AVAI-TIME-OUTA-NOT] 5.1.7.4 [AVAI-TIME-PREV-NOT] 5.1.7.5 [AVAI-TIME-NET-PRIO] 5.1.7.6 [AVAI-TIME-RES-PRIO] 5.1.7.7 [AVAI-TIME-DOS-RATE] 5.1.7.9]	U	
10	Products with digital elements minimize the negative impact by the products themselves or connected products on the availability of services provided by other products or networks.	Annex I, Part I, (2)(i)	[[AVAI-TIME-IMP-AMP] 5.1.7.8]	U	
11	Products with digital elements are designed, developed and produced to limit attack surfaces, including external interfaces.	Annex I, Part I, (2)(j)	[[LAS-INVAL] 5.1.9.1 [LAS-INSAN] 5.1.9.2 [LAS-PHY-INF] 5.1.9.3 [LAS-LOGIC-INF] 5.1.9.4 [LAS-APP] 5.1.9.5]	U	
12	Products with digital elements are designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques.	Annex I, Part I, (2)(k)	[[AVAI-TIME-RECO-POW] 5.1.7.1 [AVAI-TIME-NET-PRIO] 5.1.7.6 [AVAI-TIME-RES-PRIO] 5.1.7.7]	U	
13	Products with digital elements provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user.	Annex I, Part I, (2)(l)	[NKEV-SUM-NOTIF] 5.1.1.5	U	
14	Products with digital elements provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.	Annex I, Part I, (2)(m)	[[SDC-FRM] 5.1.2.4]	U	
15	Vulnerability handling requirements	Annex I, Part II	clause 5.2	U	

Key to columns:	
Requirement:	
No	A unique identifier for one row of the table which may be used to identify a requirement.
Description	A textual reference to the requirement.
Requirements of Regulation	Identification of article(s) defining the requirement in the Regulation.
Clause(s) of the present document	Identification of clause(s) defining the requirement in the present document unless another document is referenced explicitly.
Requirement Conditionality	
U/C	Indicates whether the requirement is unconditionally applicable (U) or is conditional upon the manufacturer's claimed functionality of the equipment (C).
Condition	Explains the conditions when the requirement is or is not applicable for a requirement which is classified "conditional".

1315

1316

1317 Annex B (informative):

1318 Guidance for the application of the present document

1319 The following approach can be used (e.g. by manufacturers)

- 1320 • to develop wearables that are compliant the present document; or
- 1321 • to analyse the compliance of a wearable to the present document.

1322 The approach is constructed such that it uses parts of an assessment of cybersecurity risks and can be integrated into the
1323 management of cybersecurity risks.

- 1324 • Step 1 - check if the wearable is in scope of the present document provided in clause 1 by:
 - 1325 - verifying that the wearable is a product as specified in the present document and within the "technical
1326 description" of the "category of product" number "17." by Regulation (EU) 2025/2392 [i.2]; and
 - 1327 - identifying the wearable context by:
 - 1328 ▪ Identify the wearable's intended use; and
 - 1329 ▪ identifying the wearable's architectural components; and
 - 1330 ▪ identifying all data processed by the wearable (data assets); and
 - 1331 ▪ identifying all functions provided by the wearable (function assets); and
 - 1332 ▪ identifying the architectural components' operational environments; and
 - 1333 ▪ identifying the architectural components' interfaces and communication types; and
 - 1334 - verifying that the wearable is covered within the product context described in clause 4 by:
 - 1335 ▪ Verify that the intended use of the wearable is covered within the product's intended purpose and
1336 foreseeable use in clause 4.1; and
 - 1337 ▪ verifying that the architectural components of the wearable are covered within the product
1338 architecture described in clause 4.5; and
 - 1339 ▪ verifying that the data processed by the wearable and the functions provided by the wearable are
1340 covered within clause 4.5; and
 - 1341 ▪ verifying that the architectural components' operational environments are covered within
1342 clause 4.6; and
 - 1343 ▪ verifying that the architectural components' interfaces and communication types are covered within
1344 clause 4.7.

1345 NOTE 1: The identification of the items mentioned above can be reused for assessing the compliance of the product
1346 with the requirements in clause 5.

1347 NOTE 2: If a product is a wearable as specified by Regulation (EU) 2025/2392 [i.1] but is not covered within the
1348 product context described in clause 4, it is assumed that the wearable is not or not completely covered by
1349 the present document. In such cases informing ETSI Technical Committee Cyber Working Group for
1350 EUSR (CYBER-EUSR) via the Committee Support Staff might help to address those wearables in
1351 potential revisions of the present document.

- 1352 • Step 2 - identify information to determine risk factors by:
 - 1353 - identifying for each function provided by the wearable:
 - 1354 ▪ its impact classes according to clause D.3; and
 - 1355 ▪ the architectural components that perform the function; and

- 1356 ▪ the communication types and the interfaces that can receive corresponding function trigger input;
1357 and
- 1358 - identifying for each data processed by the wearable:
- 1359 ▪ its impact classes according to clause D.2
- 1360 ▪ the architectural components that persistently store the data; and
- 1361 ▪ the architectural components that can communicate the data; and
- 1362 ▪ the communication types and the interfaces over which the data is communicated.

1363 NOTE 3: If data processed by the wearable or functions provided by the wearable are not covered within clause 4.1,
1364 clause C.1 can be used to identify impact classes for function and data assets that are outside the scope of
1365 the present document.

- 1366 • Step 3 - identify concrete requirements for and specific security measures/mitigations of the wearable that
1367 satisfy those requirements by:
- 1368 - for each requirement in clause 5:
- 1369 ▪ identifying the requirements applicability by evaluating the requirement's potential preconditions
1370 and exceptions based on the wearable's properties; and
- 1371 ▪ (for requirements that include assignment tables) identifying the required protection mechanisms'
1372 strengths (specified in annex E) by evaluating the requirement's assignment table based on the
1373 wearable's properties determining the attack surface and impact parameters; and
- 1374 ▪ identifying the specific security measures/mitigations that satisfy the requirement.

1375 NOTE 4: An assignment table can yield multiple mechanisms' strengths from different circumstances, which all
1376 have to be satisfied.

1377 EXAMPLE: Authentication requirements prior to changes of a wearable's configuration are different whether
1378 the changes can be made via a web GUI, accessible from adjacent or public networks, a GUI,
1379 accessible from the wearable's touchscreen, or a console, accessible by connecting to a serial port.
1380 All of this case can be simultaneously present on the same wearable.

- 1381 • Step 4 - assess the compliance of the wearable with the requirements in clause 5 by:
- 1382 - for each requirement in clause 5, performing the corresponding assessment for compliance described in
1383 clause 6 (the functional sufficiency assessments for different protection measures strengths are specified
1384 in annex E) by:
- 1385 ▪ preparing the assessment for the wearable; and
- 1386 ▪ performing the assessment activities for the wearable; and
- 1387 ▪ assigning an assessment verdict for the wearable; and
- 1388 ▪ generating the supporting evidences for the assessment.

1389 The figure B.1 provides a graphical representation of the guidance for the application of the present document.

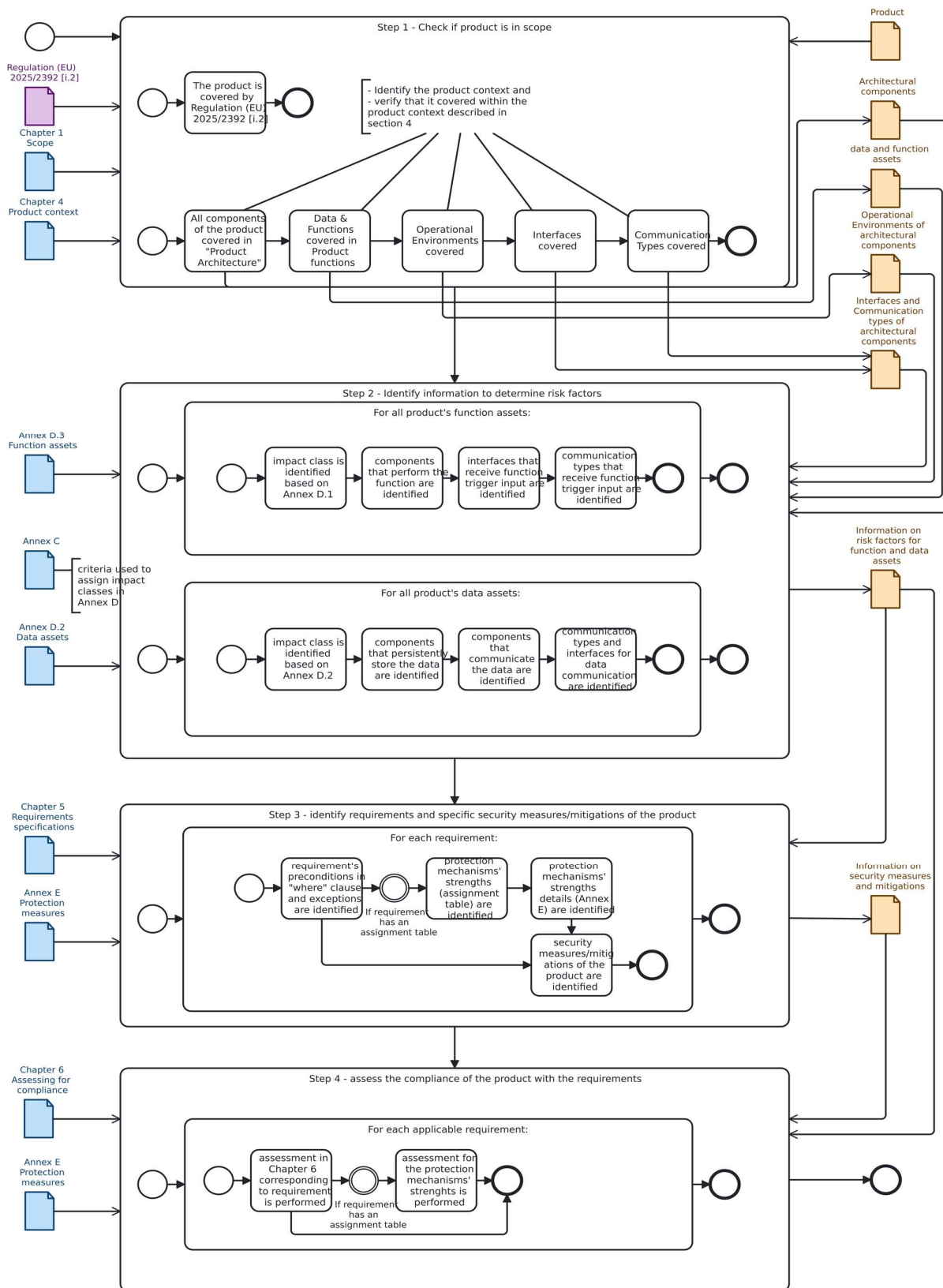


Figure B.1: Graphical representation for the application of the present document

1390

1391

1392

1393 **Annex C (informative):**
1394 **Information on the methodology for the assessment of**
1395 **cybersecurity risks used to develop the present document**

1396 **C.1 Guidance for determining impact classes**

1397 **C.1.1 General**

1398 The present document uses the following criteria to determine the impact classes of different specific wearable's assets
1399 provided in annex D.

1400 **C.1.2 Confidential data**

1401 **confidentiality impact class basic (IMP.CONF.Low):**

1402 The disclosure may lead to:

- 1403
- inconvenient consequences on the user(s); or
 - additional or increased attack opportunities over a short time and limited to communication types not higher than local on the wearable.
- 1404
- 1405

1406 **confidentiality impact class medium (IMP.CONF.Medium):**

1407 The disclosure may lead to:

- 1408
- serious impact on the user(s);
 - additional or increased attack opportunities over a short time on the wearable or
 - additional or increased attack opportunities over a prolonged time limited to non-essential functionalities on the wearable.
- 1410
- 1411

1412 **confidentiality impact class high (IMP.CONF.High):**

1413 The disclosure may lead to:

- 1414
- significant or even irreversible impact on the user(s) (e.g. personal or financial harm);
 - additional or increased attack opportunities over a prolonged time on the wearable; or
 - additional or increased attack opportunities over a short time on a significant number of wearables.
- 1415
- 1416

1417 **C.1.3 loss sensitive data**

1418 **loss sensitive availability impact class low (IMP.AVALLOSS.Low):**

1419 The loss may lead to:

- 1420
- inconvenient consequences on the user(s); or
 - non-availability of non-essential functionalities on the wearable for a short time.
- 1421

1422 **loss sensitive availability impact class medium (IMP.AVALLOSS.Medium):**

1423 The loss may lead to:

- 1424
- serious impact on the user(s); or

- 1425 • non-availability of essential functionalities of the wearable over a short time; or
- 1426 • non-availability of essential functionalities on the wearable for a prolonged time.

1427 **loss sensitive availability impact class high (IMP.AVALLOSS.High):**

1428 The loss may lead to:

- 1429 • significant or even irreversible impact on the user(s) (e.g. personal or financial harm);
- 1430 • non-availability of essential functionalities of the wearable for a prolonged time; or
- 1431 • permanent non-availability of non-essential functionalities of the wearable.

1432 **C.1.4 time sensitive data and time sensitive function**

1433 **time sensitive availability impact class low (IMP.AVAL.TIME.Low):**

1434 The delay of availability may lead to:

- 1435 • non-availability of non-essential functionalities on the wearable for a short time.

1436 **time sensitive availability impact class medium (IMP.AVAL.TIME.Medium):**

1437 The delay of availability may lead to:

- 1438 • non-availability of essential functionalities on the wearable for a short time; or
- 1439 • non-availability of non-essential functionalities on the wearable for a prolonged time.

1440 **time sensitive availability impact class high (IMP.AVAL.TIME.High):**

1441 The delay of availability may lead to:

- 1442 • non-availability of essential functionalities of the wearable for a prolonged time; or
- 1443 • permanent non-availability of non-essential functionalities of the wearable.

1444 **C.1.5 integrity relevant data and integrity relevant function**

1445 **integrity impact class low (IMP.INT.Low):**

1446 The tampering may lead to:

- 1447 • inconvenient consequences on the user(s);
- 1448 • additional or increased attack opportunities for a short time and limited to communication types not higher
- 1449 than local on the wearable; or
- 1450 • non-availability of non-essential functionalities on the wearable for a short time.

1451 **integrity impact class medium (IMP.INT.Medium):**

1452 The tampering may lead to:

- 1453 • serious impact on the user(s);
- 1454 • additional or increased attack opportunities over a short time on the wearable; or a limited number of other
- 1455 wearables;
- 1456 • additional or increased attack opportunities over a prolonged time limited to non-essential functionalities on
- 1457 the wearables; or
- 1458 • non-availability of essential functionalities on the wearable for a short time; or

1459 • non-availability of non-essential functionalities on the wearable for a prolonged time.

1460 **integrity impact class high (IMP.INT.High):**

1461 The tampering may lead to:

- 1462 • significant or even irreversible impact on the user(s) (e.g. personal or financial harm);
- 1463 • additional or increased attack opportunities for a prolonged time on the wearable or a limited number of other
- 1464 wearables;
- 1465 • additional or increased attack opportunities for a short time on a significant number of other wearables;
- 1466 • non-availability of key-functionalities of the wearables for a prolonged time; or
- 1467 • permanent non-availability of non-key-functionalities of the wearable.

1468

1469 **Annex D (normative):**
1470 **Relationship between specific data and functions assets**
1471 **covered by the present document to impact classes for**
1472 **generic asset categories**

1473 **D.1 Identifier**

1474 The following identifier for impact classes apply:

1475 **IMP:** impact class

1476 **IMP.Low:** impact class low

1477 **IMP.Medium:** impact class medium

1478 **IMP.High:** impact class high

1479 **IMP.CONF:** confidentiality impact class

1480 **IMP.CONF.Low:** confidentiality impact class low

1481 **IMP.CONF.Medium:** confidentiality impact class medium

1482 **IMP.CONF.High:** confidentiality impact class high

1483 **IMP.INT:** integrity impact class

1484 **IMP.INT.Low:** integrity impact class low

1485 **IMP.INT.Medium:** integrity impact class medium

1486 **IMP.INT.High:** integrity impact class high

1487 **IMP.AVAL.TIME:** time sensitive availability impact class

1488 **IMP.AVAL.TIME.Low:** time sensitive availability impact class low

1489 **IMP.AVAL.TIME.Medium:** time sensitive availability impact class medium

1490 **IMP.AVAL.TIME.High:** time sensitive availability impact class high

1491 **IMP.AVAL.LOSS:** loss sensitive availability impact class

1492 **IMP.AVAL.LOSS.Low:** loss sensitive availability impact class low

1493 **IMP.AVAL.LOSS.Medium:** loss sensitive availability impact class medium

1494 **IMP.AVAL.LOSS.High:** loss sensitive availability impact class high

1495 **IMP.FH:** impact class for function, whose use can cause harm

1496 **IMP.FH.Low:** function, whose use can cause harm impact class low

1497 **IMP.FH.Medium:** function, whose use can cause harm impact class medium

1498 **IMP.FH.High:** function, whose use can cause harm impact class high

1499 **IMP.FH.SP:** function, whose use can impact the safety or privacy of human entities impact class

1500 **IMP.FH.SP.Low:** function, whose use can impact the safety or privacy of human entities impact class low

1501 **IMP.FH.SP.Medium:** function, whose use can impact the safety or privacy of human entities impact class medium

- 1502 **IMP.FH.SP.High:** function, whose use can impact the safety or privacy of human entities impact class high
- 1503 **IMP.FH.DSN:** function, whose use can impact the availability of other devices, services or networks impact class
- 1504 **IMP.FH.DSN.Low:** function, whose use can impact the availability of other devices, services or networks impact class
1505 low
- 1506 **IMP.FH.DSN.Medium:** function, whose use can impact the availability of other devices, services or networks impact
1507 class medium
- 1508 **IMP.FH.DSN.High:** function, whose use can impact the availability of other devices, services or networks impact class
1509 high
- 1510 **IMP.FH.CCON:** function, which can communicate confidential data impact class
- 1511 **IMP.FH.CCON.Low:** function, which can communicate confidential data impact class low
- 1512 **IMP.FH.CCON.Medium:** function, which can communicate confidential data impact class medium
- 1513 **IMP.FH.CCON.High:** function, which can communicate confidential data impact class high
- 1514 **IMP.FH.MINT:** function, which can modify integrity relevant data impact class
- 1515 **IMP.FH.MINT.Low:** function, which can modify integrity relevant data impact class low
- 1516 **IMP.FH.MINT.Medium:** function, which can modify integrity relevant data impact class medium
- 1517 **IMP.FH.MINT.High:** function, which can modify integrity relevant data impact class high

1518

D.2 Data assets

1519

Table D.1: Mapping of specific data assets to impact classes

Specific data asset	Impact class for data asset categories			
	Impact class for confidential wearable data	Impact class for integrity relevant wearable data	Impact class for time critical availability relevant wearable data	Impact class for loss critical availability relevant wearable data
health data;	IMP.CONF.Low	IMP.INT.Low	NO	IMP.AVAI.LOSS.Low
activity data;	IMP.CONF.Low	IMP.INT.Low	NO	IMP.AVAI.LOSS.Low
input data from sensors;	NO	IMP.INT.Low	NO	IMP.AVAI.LOSS.Low
location data, including device location data;	IMP.CONF.Medium	IMP.INT.Low	NO	IMP.AVAI.LOSS.Low
location data (for children use), including device location data;	IMP.CONF.Medium	IMP.INT.High	IMP.AVAI.TIME.Medium	IMP.AVAI.LOSS.Medium
geofencing (for children use)	IMP.CONF.Medium	IMP.INT.High	IMP.AVAI.TIME.Medium	IMP.AVAI.LOSS.Medium
audio input data;	NO	NO	NO	NO
video input data;	NO	NO	NO	NO
audio output data;	IMP.CONF.Low	NO	NO	NO
video output data;	IMP.CONF.Low	NO	NO	NO
audio input data (for children use);	NO	NO	IMP.AVAI.TIME.Low	IMP.AVAI.LOSS.Low
video input data (for children use);	NO	NO	IMP.AVAI.TIME.Low	IMP.AVAI.LOSS.Low
audio output data (for children use);	IMP.CONF.Medium	IMP.INT.Low	IMP.AVAI.TIME.Low	IMP.AVAI.LOSS.Low
video output data (for children use);	IMP.CONF.Medium	IMP.INT.Low	IMP.AVAI.TIME.Low	IMP.AVAI.LOSS.Low
network status data;	NO	NO	NO	NO
access control policy data;	IMP.CONF.Medium	IMP.INT.Medium	NO	IMP.AVAI.LOSS.Medium
social interactive data	IMP.CONF.Medium	NO	NO	IMP.AVAI.LOSS.Low
social interactive data (for children use);	IMP.CONF.High	IMP.INT.Low	NO	IMP.AVAI.LOSS.Low
confidential data;	IMP.CONF.Medium	IMP.INT.Medium	NO	IMP.AVAI.LOSS.Medium
personal calendar data;	IMP.CONF.Medium	IMP.INT.Low	NO	IMP.AVAI.LOSS.Low
personal contact data;	IMP.CONF.Medium	IMP.INT.Low	NO	IMP.AVAI.LOSS.Low
personal notes data.	IMP.CONF.Medium	IMP.INT.Low	NO	IMP.AVAI.LOSS.Low

1520

1521

1522

D.3 Function assets

1523

D.3.1 Functions

1524

Table D.2: Mapping of specific function assets to impact classes for essential function asset categories

1525

Specific function asset	Impact class for function asset categories		
	Impact class for integrity relevant function	Impact class for time sensitive function	Impact class for function, whose use can cause harm
health monitoring functionalities	IMP.INT.Medium	IMP.AVAI.TIME.Medium	No
activity monitoring functionalities	IMP.INT.Low	IMP.AVAI.TIME.Low	No
positioning functionalities	IMP.INT.Low	IMP.AVAI.TIME.Low	No
location sharing functionalities	IMP.INT.Medium	IMP.AVAI.TIME.Medium	No
emergency location functionalities	IMP.INT.High	IMP.AVAI.TIME.High	IMP.FH.High
location sharing functionalities (for children use)	IMP.INT.High	IMP.AVAI.TIME.High	IMP.FH.High
parental control functionalities	IMP.INT.High	IMP.AVAI.TIME.High	IMP.FH.High
audio input functionalities	IMP.INT.Low	IMP.AVAI.TIME.Low	No
audio input functionalities (for children use)	IMP.INT.High	IMP.AVAI.TIME.Medium	IMP.FH.Low
video input functionalities	IMP.INT.Low	IMP.AVAI.TIME.Low	No
video input functionalities (for children use)	IMP.INT.High	IMP.AVAI.TIME.Medium	IMP.FH.Low
notification functionalities	IMP.INT = IMP.INT of the function who generated the notification	IMP.AVAI.TIME = IMP.AVAI.TIME of the function who generated the notification	IMP.FH = IMP.FH of the function who generated the notification
audio output functionalities	IMP.INT.Low	IMP.AVAI.TIME.Low	No
audio output functionalities (for children use)	IMP.INT.High	IMP.AVAI.TIME.Medium	IMP.FH.Low
video output functionalities	IMP.INT.Low	IMP.AVAI.TIME.Low	No
video output functionalities (for children use)	IMP.INT.High	IMP.AVAI.TIME.Medium	IMP.FH.Low
functionalities which can communicate wearable data assets	IMP.INT = Maximum (IMP.CONF, IMP.INT) of communicated data	IMP.AVAI.TIME = IMP.AVAI.TIME of communicated data	IMP.FH = Maximum (IMP.FH.Low, IMP.CONF of communicated data)

1526

1527 **D.3.2 Functions whose use can cause harm**

1528 The contents of the column *impact class for function, whose use can cause harm* of table D.3 are split into details in
 1529 table D.4.

1530 **Table D.3: Mapping of specific function assets to impact classes for different aspects of function,**
 1531 **whose use can cause harm**

Specific function asset	Impact class for function, whose use can impact the safety or privacy of human entities	Impact class for function, whose use can impact the availability of other devices, services or networks	Impact class for function, which can communicate confidential data	Impact class for function, which can modify integrity relevant data
emergency location functionalities	IMP.FH.SP.High	NO	IMP.FH.CCON = IMP.CONF of communicated control data	IMP.FH.SP.Medium
location sharing functionalities (for children use)	IMP.FH.SP.High	NO	IMP.FH.CCON = IMP.CONF of communicated control data	IMP.FH.SP.Medium
parental control functionalities	IMP.FH.SP.High	NO	NO	NO
audio input functionalities (for children use)	IMP.FH.SP.Low	NO	NO	NO
video input functionalities (for children use)	IMP.FH.SP.Low	NO	NO	NO
notification functionalities	IMP.FH.SP = IMP.FH.SP of the function who generated the notification	NO	NO	NO
audio output functionalities (for children use)	IMP.FH.SP.Low	NO	NO	NO
video output functionalities (for children use)	IMP.FH.SP.Low	NO	NO	NO
functionalities which can communicate wearable data assets	NO	IMP.FH.DSN.Low	IMP.FH.CCON = IMP.CONF of communicated control data	NO

1532

1533

1534

1535

1536 **Annex E (normative):**
1537 **Protection measures**

1538 **E.1 Identifier**

1539 The following identifier apply here and in the assignment tables in clause 5:

1540 **N/A:** not applicable

1541 **AUTH.Basic:** authentication strength level basic

1542 **AUTH.Normal:** authentication strength level normal

1543 **AUTH.Enhanced:** authentication strength level enhanced

1544 **AUTH.Strong:** authentication strength level strong

1545 **CONF.COM.Basic:** communication of confidential data protection strength level basic

1546 **CONF.COM.Normal:** communication of confidential data protection strength level normal

1547 **CONF.COM.Enhanced:** communication of confidential data protection strength level enhanced

1548 **CONF.COM.Strong:** communication of confidential data protection strength level strong

1549 **INT.COM.Basic:** communication of integrity relevant data protection strength level basic

1550 **INT.COM.Normal:** communication of integrity relevant data protection strength level normal

1551 **INT.COM.Enhanced:** communication of integrity relevant data protection strength level enhanced

1552 **INT.COM.Strong:** communication of integrity relevant data protection strength level strong

1553 **CONF.SSM.Basic:** confidential persistent storage strength level basic

1554 **CONF.SSM.Normal:** confidential persistent storage strength level normal

1555 **CONF.SSM.Enhanced:** confidential persistent storage strength level enhanced

1556 **CONF.SSM.Strong:** confidential persistent storage strength level strong

1557 **SAN.Normal:** input sanitization of input strength level normal

1558 **SAN.Strong:** input sanitization of input strength level strong

1559 **AUT.VER.Enhanced:** authenticity verification strength level enhanced

1560 **AUT.VER.Strong:** authenticity verification strength level strong

1561 **INT.SW.VER.Basic:** software package integrity verification strength level basic

1562 **INT.SW.VER.Normal:** software package integrity verification strength level normal

1563 **INT.SW.VER.Enhanced:** software package integrity verification strength level enhanced

1564 **INT.SW.VER.Strong:** software package integrity verification strength level strong

1565 **INT.VER.Basic:** integrity verification strength level basic

1566 **INT.VER.Normal:** integrity verification strength level normal

1567 **INT.VER.Enhanced:** integrity verification strength level enhanced

1568 **INT.VER.Strong:** integrity verification strength level strong

1569 E.2 access control mechanism's strength

1570 E.3 authentication mechanism strength

1571 E.3.1 AUM-FH Authentication for functions whose use can cause
1572 harm

1573 E.3.1.1 General

1574 The present document specifies the strength of authentication mechanisms by their resistance against certain attack
1575 types. Those attack types are constructed such that mechanisms of higher strength protect against all attack types
1576 required for lower strengths.

1577 E.3.1.2 Authentication strength level basic

1578 The authentication strength level basic shall protect against the following attack types:

1579 **limited presentation attack:** Opportunistic presentation attacks on authentication mechanisms based on authentication
1580 factors of the type inherence, using authentication factors of another entity

1581 **limited brute force attack:** Opportunistic guessing attacks on authentication mechanisms based on authentication
1582 factors of the type knowledge, by guessing manually without the use of technical aids.

1583 E.3.1.3 Authentication strength level medium

1584 The authentication strength level medium shall protect against the following attack types:

1585 **automated brute force attack:** Brute force attacks on authentication mechanisms based on authentication factors of the
1586 type knowledge, by systematic try out with technical.

1587 **presentation attack:** Presentation attacks on authentication mechanisms based on authentication factors of the type
1588 inherence, using medium effort methods like e.g. photos, cut out masks, audio replays, video replays, AI generated
1589 voices

1590 **automated security token spoofing attack:** Security token spoofing attacks on authentication mechanisms based on
1591 authentication factors of the type possession, by using authentication factors sourced from other uses or self-created,
1592 without using any specific knowledge of the targeted authentication mechanisms.

1593 **replay attack:** An attacker intercepts valid data transmission and retransmits them to mimic the original communication
1594 partner for accepting an authentication based on the authentication factors of the type knowledge or possession (e.g. a
1595 session token).

1596 **person in the middle attack:** An attacker secretly intercepts and alters the authentication between two parties who
1597 believe they are communicating directly with each other based on the authentication factors of the type knowledge or
1598 possession (e.g. a session token).

1599 E.3.1.4 Authentication strength level enhanced

1600 The authentication strength level enhanced shall protect against the following attack types:

1601 **targeted presentation attack:** Presentation attacks on authentication mechanisms based on authentication factors of the
1602 type inherence, using enhanced effort methods like e.g. (partial) silicone masks, layered prints.

1603 **targeted brute force attack:** Brute force attacks on authentication mechanisms based on authentication factors of the
1604 type knowledge, by systematic try out with technical aids, making use of target specific information.

1605 **targeted security token spoofing attack:** Security token spoofing attacks on authentication mechanisms based on
1606 authentication factors of the type possession, by using authentication factors sourced from devices of the same type as
1607 the wearable or self-created, using specific knowledge of the targeted authentication mechanisms and the wearable.

1608 **replay attack:** An attacker intercepts valid data transmission and retransmits them to mimic the original communication
1609 partner for accepting an authentication based on the authentication factors of the type knowledge or possession (e.g. a
1610 session token).

1611 **person in the middle attack:** An attacker secretly intercepts and alters the authentication between two parties who
1612 believe they are communicating directly with each other based on the authentication factors of the type knowledge or
1613 possession (e.g. a session token).

1614 E.3.1.5 Authentication strength level strong

1615 The authentication strength level strong shall protect against the following attack types:

1616 **elaborate presentation attack:** Presentation attacks on authentication mechanisms based on authentication factors of
1617 the type inheritance", using high effort methods like e.g. highly realistic silicone or latex masks, limb replicas, trained
1618 deep fakes.

1619 **elaborate brute force attack:** Brute force attacks on authentication mechanisms based on authentication factors of the
1620 type knowledge, by systematic try out with technical aids, making use of target specific information, and unrestricted
1621 duration.

1622 **elaborate security token spoofing attack:** Security token spoofing attacks on authentication mechanisms based on
1623 authentication factors of the type possession, by using authentication factors created or sourced from devices of the
1624 same type as the wearable and modified, specifically for the targeted authentication mechanisms.

1625 **replay attack:** An attacker intercepts valid data transmission and retransmits them to mimic the original communication
1626 partner for accepting an authentication based on the authentication factors of the type knowledge or possession (e.g. a
1627 session token).

1628 **person in the middle attack:** An attacker secretly intercepts and alters the authentication between two parties who
1629 believe they are communicating directly with each other based on the authentication factors of the type knowledge or
1630 possession (e.g. a session token).

1631 E.3.2 Assessment for authentication mechanism strength

1632 E.3.2.1 Assessment criteria regarding the protection against limited 1633 presentation attacks

1634 **Assessment objective:**

1635 The assessment covers functional testing of authentication mechanisms that provide a basic level of protection and use
1636 authentication factors of the type inheritance against limited presentation attacks.

1637 **Assessment preparation:**

- 1638 • the wearable shall be set up in default configuration;
- 1639 • a genuine enrolled biometric template in the corresponding authentication mechanism with credential for
1640 authentication shall be created;
- 1641 • at least one interface, where the authentication mechanism is reachable shall be documented.

1642 **Assessment activities:**

- 1643 • authentication at the created genuine enrolled biometric template shall be attempted using the correct genuine
1644 enrolled biometric template identifier, if present, and authentication factors, not belonging to the person who
1645 set up the account, for at least five times or ten minutes at highest archivable query frequency;
- 1646 • the outcome and used authentication factor of each attempt shall be recorded.

1647 **Assignment of verdict:**

1648 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts.

1649 The verdict FAIL shall be assigned otherwise.

1650 **Supporting Evidence:**

- 1651 • description of the performed test;
- 1652 • all test records of the performed test.

1653 **E.3.2.2 Assessment criteria regarding the protection against targeted**
1654 **presentation attacks**

1655 **Assessment objective:**

1656 The assessment covers functional testing of authentication mechanisms that provide a enhanced level of protection and
1657 use authentication factors of the type inherence against targeted presentation attacks.

1658 **Assessment preparation:**

- 1659 • the wearable shall be set up in default configuration
- 1660 • a genuine enrolled biometric template in the corresponding authentication mechanism with credential for
1661 authentication shall be created;
- 1662 • at least one interface, where the authentication mechanism is reachable shall be documented;
- 1663 • authentication factors shall be fabricated using common materials and tools as well as readily available source
1664 materials. The fabrication process shall not be longer than *one workday* per authentication factor.

1665 **Assessment activities:**

- 1666 • authentication at the created genuine enrolled biometric template shall be attempted using the correct genuine
1667 enrolled biometric template identifier, if present, and at least two fabricated authentication factors tried at least
1668 five times with slightly different parameters each;
- 1669 • the outcome and used authentication factor of each attempt shall be recorded.

1670 **Assignment of verdict:**

1671 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts.

1672 The verdict FAIL shall be assigned otherwise.

1673 **Supporting Evidence:**

- 1674 • description of the performed test;
- 1675 • all test records of the performed test.

1676 **E.3.2.3 Assessment criteria regarding the protection against elaborate**
1677 **presentation attacks**

1678 **Assessment objective:**

1679 The assessment covers functional testing of authentication mechanisms that provide a high level of protection and use
1680 authentication factors of the type inherence against elaborate presentation attacks.

1681 **Assessment preparation:**

- 1682 • the wearable shall be set up in default configuration;

- 1683 • a genuine enrolled biometric template in the corresponding authentication mechanism with credential for
1684 authentication shall be created;
- 1685 • at least one interface, where the authentication mechanism is reachable shall be documented;
- 1686 • authentication factors shall be fabricated using specialized materials and tools as well as cumbersome
1687 extracted source materials. The duration of the fabrication process per authentication factor is not restricted.

1688 **Assessment activities:**

- 1689 • authentication at the created genuine enrolled biometric template shall be attempted using the correct genuine
1690 enrolled biometric template identifier, if present, and at least two fabricated authentication factors tried at least
1691 five times with slightly different parameters each;
- 1692 • the outcome and used authentication factor of each attempt shall be recorded.

1693 **Assignment of verdict:**

1694 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts.

1695 The verdict FAIL shall be assigned otherwise.

1696 **Supporting Evidence:**

- 1697 • description of the performed test;
- 1698 • all test records of the performed test.

1699 **E.3.2.4 Assessment criteria regarding the protection against limited brute**
1700 **force attacks**

1701 **Assessment objective:**

1702 The assessment covers functional testing of authentication mechanisms that provide a basic level of protection and use
1703 authentication factors of the type knowledge against limited brute force attacks.

1704 **Assessment preparation:**

- 1705 • the wearable shall be set up in default configuration;
- 1706 • at least one interface, where the authentication mechanism is reachable shall be documented;
- 1707 • the security insurance time (T_{SI}) for this assessment is 10 minutes (600 s).

1708 **Assessment activities:**

- 1709 • the minimal recommended complexity of passwords accepted by the mechanism ($C_{PW,min}$) shall be
1710 determined; e.g. $C_{PW,min} = (10)^6$ for a 6-digit PIN or $C_{PW,min} = \frac{9!}{(9-5)!}$ for a pattern of 5 nonrecurring nodes in
1711 a field of 9 notes;
- 1712 • the maximum sustained login attempt frequency ($f_{LA,max}$) shall be determined; e.g. $f_{LA,max} = \frac{5}{5 \times 3s + 3600s}$ for 3
1713 seconds per login attempt + a one-hour waiting period after 5 failed login attempts;
- 1714 • the probability of guessing a completely random password of the minimal recommended complexity (p_{GRP})
1715 shall be calculated by $p_{GRP} = T_{SI} * f_{LA,max} / C_{PW,min}$;
- 1716 • the methods and outcome of each step shall be recorded.

1717 **Assignment of verdict:**

1718 The verdict PASS shall be assigned if the calculated probability p_{GRP} is less than 10^{-2} .

1719 The verdict FAIL shall be assigned otherwise.

1720 **Supporting Evidence:**

- 1721 • the authentication mechanism and the interface via which it was accessed;
- 1722 • all test records of the performed test.

1723 **E.3.2.5 Assessment criteria regarding the protection against targeted brute**
1724 **force attacks**1725 **Assessment objective:**

1726 The assessment covers functional testing of authentication mechanisms that provide an enhanced level of protection and
1727 use authentication factors of the type knowledge against targeted brute force attacks.

1728 **Assessment preparation:**

- 1729 • the wearable shall be set up in default configuration;
- 1730 • at least one interface, where the authentication mechanism is reachable shall be documented;
- 1731 • the security insurance time (T_{SI}) for this assessment one month ($2,6 * 10^6s$).

1732 **Assessment activities:**

- 1733 • the minimal recommended complexity of passwords accepted by the mechanism ($C_{PW,min}$) shall be
1734 determined; e.g. $C_{PW,min} = (26 * 2 + 10)^8$ for minimum 8 characters of upper-case or lower-case letters or
1735 numbers.
- 1736 • the maximum sustained login attempt frequency ($f_{LA,max}$) shall be determined; e.g. $f_{LA,max} = (0,1 s)^{-1}$ for 10
1737 login attempt per second.
- 1738 • the probability of guessing a completely random password of the minimal recommended complexity (p_{GRP})
1739 shall be calculated by $p_{GRP} = T_{SI} * f_{LA,max} / C_{PW,min}$.
- 1740 • the methods and outcome of each step shall be recorded.

1741 **Assignment of verdict:**

1742 The verdict PASS shall be assigned if the calculated probability p_{GRP} is less than 10^{-6} .
1743 The verdict FAIL shall be assigned otherwise.

1744 **Supporting Evidence:**

- 1745 • the authentication mechanism and the interface via which it was accessed;
- 1746 • all test records of the performed test.

1747 **E.3.2.6 Assessment criteria regarding the protection against automated**
1748 **brute force attacks**1749 **Assessment objective:**

1750 The assessment covers functional testing of authentication mechanisms that provide a medium level of protection and
1751 use authentication factors of the type knowledge against targeted brute force attacks.

1752 **Assessment preparation:**

- 1753 • the wearable shall be set up in default configuration;
- 1754 • at least one interface, where the authentication mechanism is reachable shall be documented;
- 1755 • the security insurance time (T_{SI}) for this assessment is one day (86 400 s).

1756 **Assessment activities:**

- 1757 • the minimal recommended complexity of passwords accepted by the mechanism ($C_{PW,min}$) shall be
1758 determined; e.g. $C_{PW,min} = (26 * 2 + 10)^8$ for minimum 8 characters of upper-case case or lower-case letters
1759 or numbers;
- 1760 • the maximum sustained login attempt frequency ($f_{LA,max}$) shall be determined; e.g. $f_{LA,max} = \frac{5}{5 \times 3s + 3600}$ for 3
1761 seconds per login attempt + a one-hour waiting period after 5 failed login attempts;
- 1762 • the probability of guessing a completely random password of the minimal recommended complexity (p_{GRP})
1763 shall be calculated by $p_{GRP} = T_{SI} * f_{LA,max} / C_{PW,min}$;
- 1764 • the methods and outcome of each step shall be recorded.

1765 **Assignment of verdict:**

1766 The verdict PASS shall be assigned if the calculated probability p_{GRP} is less than 10^{-6} .

1767 The verdict FAIL shall be assigned otherwise.

1768 **Supporting Evidence:**

- 1769 • the authentication mechanism and the interface via which it was accessed;
- 1770 • all test records of the performed test.

1771 E.3.2.7 Assessment criteria regarding the protection against presentation 1772 attacks

1773 **Assessment objective:**

1774 The assessment covers functional testing of authentication mechanisms that provide a medium level of protection and
1775 use authentication factors of the type inherence against presentation attacks.

1776 **Assessment preparation:**

- 1777 • the wearable shall be set up in default configuration;
- 1778 • a genuine enrolled biometric template in the corresponding authentication mechanism with credential for
1779 authentication shall be created;
- 1780 • at least one interface, where the authentication mechanism is reachable shall be documented;
- 1781 • authentication factors shall be fabricated using readily available materials and tools as well as readily available
1782 source materials. The fabrication process shall not be longer than *twenty* minutes per authentication factor.

1783 NOTE: Readily available source materials are e.g. fingerprints on everyday items or publicly available photos.
1784 Readily available materials and tools are of adhesive tape, printer paper, common printers.

1785 **Assessment activities:**

- 1786 • authentication at the created account shall be attempted using the correct account name, if present, and at least
1787 two fabricated authentication factors tried at least five times with slightly different parameters each;
- 1788 • the outcome and used fabricated authentication factor of each attempt shall be recorded.

1789 **Assignment of verdict:**

1790 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts.

1791 The verdict FAIL shall be assigned otherwise.

1792 **Supporting Evidence:**

- 1793 • description of the performed test

- 1794
- all test records of the performed test

1795 E.3.2.8 Assessment criteria regarding the protection against elaborate brute 1796 force attacks

1797 **Assessment objective:**

1798 The assessment covers functional testing of authentication mechanisms that provide a high level of protection and use
1799 authentication factors of the type knowledge against targeted brute force attacks.

1800 **Assessment preparation:**

- 1801
- the wearable shall be set up in default configuration;

1802

 - at least one interface, where the authentication mechanism is reachable shall be documented;

1803

 - the security insurance time (T_{SI}) for this assessment is five years ($1,6 * 10^8 s$).

1804 **Assessment activities:**

- 1805
- the minimal recommended complexity of passwords accepted by the mechanism ($C_{PW,min}$) shall be
1806 determined; e.g. $(26x2 + 10)^8$ for minimum 8 characters of upper-case case or lower-case letters or numbers;

1807

 - the maximum sustained login attempt frequency ($f_{LA,max}$) shall be determined; e.g. $(0,1s)^{-1}$ for 10 login
1808 attempt per second;

1809

 - the probability of guessing a completely random password of the minimal recommended complexity (p_{GRP})
1810 shall be calculated by $p_{GRP} = T_{SI} \times f_{LA,max} / C_{PW,min}$;

1811

 - the methods and outcome of each step shall be recorded.

1812 **Assignment of verdict:**

1813 The verdict PASS shall be assigned if the calculated probability is less than 10^{-6} .

1814 The verdict FAIL shall be assigned otherwise.

1815 **Supporting Evidence:**

- 1816
- the authentication mechanism and the interface via which it was accessed;

1817

 - all test records of the performed test.

1818 E.3.2.9 Assessment criteria regarding the protection against automated 1819 security token spoofing attacks

1820 **Assessment objective:**

1821 The assessment covers functional testing of authentication mechanisms that provide a medium level of protection and
1822 use authentication factors of the type possession against automated security token spoofing attacks.

1823 **Assessment preparation:**

- 1824
- the wearable shall be set up in default configuration;

1825

 - an account in the corresponding authentication mechanism with a security token for authentication shall be
1826 created;

1827

 - at least one interface, where the authentication mechanism is reachable shall be documented;

1828

 - security tokens, that match specifications of the interfaces, via which the authentication mechanism is
1829 reachable, shall be prepared or created without using any specific knowledge of the authentication mechanism.

1830 **Assessment activities:**

1831 • authentication at the created account shall be attempted using the correct account name, if present, and the
1832 prepared or created security tokens;

1833 • the outcome and used authentication factor of each attempt shall be recorded.

1834 **Assignment of verdict:**

1835 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts, except where the used
1836 authentication factor exactly matches the configured one.

1837 The verdict FAIL shall be assigned otherwise.

1838 **Supporting Evidence:**

1839 • description of the performed test;

1840 • all test records of the performed test.

1841 **E.3.2.10 Assessment criteria regarding the protection against targeted**
1842 **security token spoofing attacks**

1843 **Assessment objective:**

1844 The assessment covers functional testing of authentication mechanisms that provide an enhanced level of protection and
1845 use authentication factors of the type possession against targeted security token spoofing attacks.

1846 **Assessment preparation:**

1847 • the wearable shall be set up in default configuration;

1848 • an account in the corresponding authentication mechanism with a security token for authentication shall be
1849 created;

1850 • at least one interface, where the authentication mechanism is reachable shall be documented;

1851 • security tokens, shall be prepared or created, which match the specifications of the authentication mechanism.

1852 **Assessment activities:**

1853 • authentication at the created account shall be attempted using the correct account name, if present, and the
1854 prepared or created security tokens;

1855 • the outcome and used authentication factor of each attempt shall be recorded.

1856 **Assignment of verdict:**

1857 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts, except where the used
1858 authentication factor exactly matches the configured one.

1859 The verdict FAIL shall be assigned otherwise.

1860 **Supporting Evidence:**

1861 • description of the performed test;

1862 • all test records of the performed test.

1863 **E.3.2.11 Assessment criteria regarding the protection against elaborate**
1864 **security token spoofing attacks**

1865 **Assessment objective:**

1866 The assessment covers functional testing of authentication mechanisms that provide a high level of protection and use
1867 authentication factors of the type possession against elaborate security token spoofing attacks.

1868 Assessment preparation:

- 1869 • the wearable shall be set up in default configuration;
- 1870 • an account in the corresponding authentication mechanism with a security token for authentication shall be
1871 created;
- 1872 • at least one interface, where the authentication mechanism is reachable shall be documented;
- 1873 • security tokens, shall be prepared or created, which match the specifications of the authentication mechanism
1874 and use information extracted from the original security token.

1875 Assessment activities:

- 1876 • authentication at the created account shall be attempted using the correct account name, if present, and the
1877 prepared or created security tokens;
- 1878 • the outcome and used authentication factor of each attempt shall be recorded.

1879 Assignment of verdict:

1880 The verdict PASS shall be assigned if the authentication mechanism rejects all attempts, except where the used
1881 authentication factor exactly matches the configured one.

1882 The verdict FAIL shall be assigned otherwise.

1883 Supporting Evidence:

- 1884 • description of the performed test.
- 1885 • all test records of the performed test.

1886 E.3.2.12 Assessment criteria regarding the protection against replay attacks**1887 Assessment objective:**

1888 The assessment covers functional testing of authentication mechanisms that use authentication factors of the type
1889 knowledge or possession (e.g. a session token) against replay attacks.

1890 Assessment preparation:

- 1891 • the wearable shall be set up in default configuration;
- 1892 • the authentication mechanism shall be active;
- 1893 • a communication partner with active authentication mechanisms shall be set up for the wearable;
- 1894 • a capture and replay tool between wearable and its communication partner shall be set up;
- 1895 • at least one interface, where the authentication mechanism is reachable shall be documented.

1896 Assessment activities:

- 1897 • Initiate a connection between the wearable and its communication partner.
- 1898 • Use a capture tool to record the transmitted message or transaction data.
- 1899 • Replay (retransmit) the captured message to the wearable using a suitable tool in place to mimic the original
1900 communication partner.
- 1901 • Record if the wearable accepts the retransmitted data.

1902 Assignment of verdict:

1903 The verdict PASS shall be assigned if it is not possible to impersonate as the communication partner.

1904 The verdict FAIL shall be assigned otherwise.

1905 **Supporting Evidence:**

- 1906 • description of the performed test;
- 1907 • all test records of the performed test.

1908 E.3.2.13 Assessment criteria regarding the protection against PitM attacks

1909 **Assessment objective:**

1910 The assessment covers functional testing of authentication mechanisms that use authentication factors of the type
1911 knowledge or possession (e.g. a session token) against PitM attacks.

1912 **Assessment preparation:**

- 1913 • the wearable shall be set up in default configuration;
- 1914 • the authentication mechanism shall be active;
- 1915 • a communication partner with active authentication mechanisms shall be set up for the wearable;
- 1916 • a capture and PitM tool between wearable and its communication partner shall be set up;
- 1917 • at least one interface, where the authentication mechanism is reachable shall be documented.

1918 **Assessment activities:**

- 1919 • Initiate a connection between the wearable and its communication partner.
- 1920 • Attempt to capture data (consumer credentials, tokens, etc.) with the tool in place and actively intercept
1921 communication to impersonate the communication partner during:
 - 1922 - generation and communication of authentication factors for the communication partner (if not pre-
1923 configured); and
 - 1924 - authentication of the communication partner.
- 1925 • Record if the impersonation as communication partner is successful.

1926 **Assignment of verdict:**

1927 The verdict PASS shall be assigned if it is not possible to impersonate as the communication partner.

1928 The verdict FAIL shall be assigned otherwise.

1929 **Supporting Evidence:**

- 1930 • description of the performed test;
- 1931 • all test records of the performed test.

1932 E.4 confidentiality protection strength

1933 E.4.1 CONF-SSM Confidentiality protecting persistent storage for 1934 confidential data

1935 E.4.1.1 General

1936 The present document specifies confidentiality protecting secure storage mechanisms' strength, by certain security
1937 properties. Those properties are constructed such that mechanisms of higher strength have the properties of lower
1938 strength mechanisms.

1939 E.4.1.2 confidential persistent storage strength level basic

1940 Mechanisms for the confidential persistent storage strength level basic shall encrypt such that decryption is only
1941 possible for the wearable.

1942 E.4.1.3 confidential persistent storage strength level medium

1943 Mechanisms for the confidential persistent storage strength level medium shall encrypt such that decryption is

- 1944
- only possible for the wearable; and
 - only performed after a successful authentication.
- 1945

1946 E.4.1.4 confidential persistent storage strength level enhanced

1947 Mechanisms for the confidential persistent storage strength level enhanced shall encrypt supported by hardware, such
1948 that:

- 1949
- decryption is only possible for the wearable after a successful authentication; and
 - the extraction of the encryption key is prevented by hardware.
- 1950

1951 E.4.1.5 confidential persistent storage strength level strong

1952 Mechanisms for the confidential persistent storage strength level strong shall prevent the extraction of data by hardware.

1953 E.5 confidentiality protection strength

1954 E.5.1 CONF-COM Communication of confidential data

1955 E.5.1.1 General

1956 The present document specifies the strength of mechanisms to protect the confidentiality of communicated confidential
1957 data by their resistance against certain attack types. Those attack types are constructed such that mechanisms of higher
1958 strength protect against all attack types required for lower strengths.

1959 E.5.1.2 communication of confidential data protection strength level basic

1960 The communication of confidential data protection strength level basic shall protect against the following attack types:

1961 **eavesdropping:** An attacker secretly intercepts the communication between the wearable and another entity or another
1962 part of the wearable.

1963 E.5.1.3 communication of confidential data protection strength level medium

1964 The communication of confidential data protection strength level normal shall protect against the following attack
1965 types:

1966 **eavesdropping**: An attacker secretly intercepts the communication between the wearable and another entity or another
1967 part of the wearable.

1968 **direct identity spoofing attack**: An attacker mimics another entity to gain a trust relationship with the wearable

1969 **downgrade of communication protocols attack**: An attacker forces to use of a legacy, less secure, communication
1970 protocol

1971 E.5.1.4 communication of confidential data protection strength level 1972 enhanced

1973 The communication of confidential data protection strength level enhanced shall protect against the following attack
1974 types:

1975 **eavesdropping**: An attacker secretly intercepts the communication between the wearable and another entity or another
1976 part of the wearable.

1977 **person in the middle attack**: An attacker secretly alters the communication between the wearable and another entity or
1978 another part of the wearable to gain a trusted relationship with the involved communication partners without their
1979 knowledge.

1980 **direct identity spoofing attack**: An attacker mimics another entity to gain a trust relationship with the wearable

1981 **downgrade of communication protocols attack**: An attacker forces to use of a legacy, less secure, communication
1982 protocol

1983 E.5.1.5 communication of confidential data protection strength level strong

1984 The communication of confidential data protection strength level strong shall protect against the following attack types:

1985 **eavesdropping**: An attacker secretly intercepts the communication between the wearable and another entity or another
1986 part of the wearable.

1987 **person in the middle attack**: An attacker secretly alters the communication between the wearable and another entity or
1988 another part of the wearable to gain a trusted relationship with the involved communication partners without their
1989 knowledge.

1990 **direct identity spoofing attack**: An attacker mimics another entity to gain a trust relationship with the wearable

1991 **downgrade of communication protocols attack**: An attacker forces to use of a legacy, less secure, communication
1992 protocol

1993 E.6 integrity protection strength

1994 E.6.1 INT-SWPCK Software package verification

1995 E.6.1.1 General

1996 The present document specifies software package verification mechanisms' strength, by certain protection measures.
1997 Those measures are constructed such that measures of higher strength typically have less attack vectors than lower
1998 strength measures.

1999 E.6.1.2 software package integrity verification strength level basic

2000 Mechanisms for the software package integrity verification strength level basic shall:

- 2001 • explicitly obtain the confirmation of an authorized entity that the integrity and authenticity of a software
2002 package has been verified by the entity, where the software package's source is determined by the entity; or
- 2003 • explicitly obtain the confirmation of an authorized entity that the authenticity of a software package has been
2004 verified by the entity and use a hash or checksum provided by the entity for the software package to verify its
2005 integrity, where the software package's source is determined by the entity.
- 2006 **E.6.1.3 software package integrity verification strength level medium**
- 2007 Mechanisms for the software package integrity verification strength level normal shall ensure that a software package
2008 has been obtained from a trusted source over a secure communication channel that meets INT.COM.Enhanced.
- 2009 **E.6.1.4 software package integrity verification strength level enhanced**
- 2010 Mechanisms for the software package integrity verification strength level enhanced shall verify the authenticity and
2011 integrity of a software package using cryptographic digital signature verification.
- 2012 **E.6.2 INT-COM Communication of integrity relevant data**
- 2013 **E.6.2.1 General**
- 2014 The present document specifies the strength of mechanisms to protect the integrity of communicated integrity relevant
2015 data by their resistance against certain attack types. Those attack types are constructed such that mechanisms of higher
2016 strength protect against all attack types required for lower strengths.
- 2017 **E.6.2.2 communication of integrity relevant data protection strength level basic**
- 2018 The communication of integrity relevant data protection strength level basic shall protect against the following attack
2019 types:
- 2020 **accidental bit flip:** Accidental change of data by natural causes.
- 2021 **E.6.2.3 communication of integrity relevant data protection strength level medium**
- 2022 The communication of integrity relevant data protection strength level normal shall protect against the following attack
2023 types:
- 2024 **replay attack:** An attacker intercepts valid transmissions and then retransmits those captured messages to the same
2025 interface to deceive it into performing unauthorized actions.
- 2026 **accidental bit flip:** Accidental change of data by natural causes.
- 2027 **direct identity spoofing attack:** An attacker mimics another entity to gain a trust relationship with the wearable
- 2028 **downgrade of communication protocols attack:** An attacker forces to use of a legacy, less secure, communication
2029 protocol
- 2030 **E.6.2.4 communication of integrity relevant data protection strength level enhanced**
- 2031 The communication of integrity relevant data protection strength level enhanced shall protect against the following
2032 attack types:
- 2033 **replay attack:** An attacker intercepts valid transmissions and then retransmits those captured messages to the same
2034 interface to deceive it into performing unauthorized actions.
- 2035 **person in the middle attack:** An attacker secretly alters the communication between the wearable and another entity or
2036 another part of the wearable to gain a trusted relationship with the involved communication partners without their
2037 knowledge.
- 2038 **accidental bit flip:** Accidental change of data by natural causes.

2039 **direct identity spoofing attack:** An attacker mimics another entity to gain a trust relationship with the wearable.

2040 **downgrade of communication protocols attack:** An attacker forces to use of a legacy, less secure, communication
2041 protocol.

2042 E.6.2.5 communication of integrity relevant data protection strength level strong

2043 The communication of integrity relevant data protection strength level strong shall protect against the following attack
2044 types:

2045 **replay attack:** An attacker intercepts valid transmissions and then retransmits those captured messages to the same
2046 interface to deceive it into performing unauthorized actions.

2047 **person in the middle attack:** An attacker secretly alters the communication between the wearable and another entity or
2048 another part of the wearable to gain a trusted relationship with the involved communication partners without their
2049 knowledge.

2050 **accidental bit flip:** Accidental change of data by natural causes.

2051 **direct identity spoofing attack:** An attacker mimics another entity to gain a trust relationship with the wearable.

2052 **downgrade of communication protocols attack:** An attacker forces to use of a legacy, less secure, communication
2053 protocol.

2054

2055
2056
2057
2058
2059
2060
2061

Annex F (informative): Relationship between the present document and the covered/not covered cybersecurity risks

Table [F.1](#) shows the threat scenarios considered, the mitigation measures related to them in the present document with associated attack surface parameters, and the risk coverage.

Table F.1: Covered threats and remaining risks acceptance

No.	Threat Actor	Threat action	Asset	Threat details		Requirement(s) for mitigation	Relevant attack surface parameter	Risk coverage
[1]	A threat actor	(mis)uses	a function whose use can cause harm	on the wearable		Prevention: [ACM-FH] 5.1.3.1 [AUM-FH] 5.1.3.2 [AUTHZ-LP] 5.1.3.3 [AUTHZ-R] 5.1.3.4 [AVAI-TIME-IMP-AMP] 5.1.7.8 [LAS-PHY-INF] 5.1.9.3 [LAS-LOGIC-INF] 5.1.9.4 [LAS-APP] 5.1.9.5 [SDC-AUM-FH] 5.1.2.1 Information: Restoration: [SDC-FRM] 5.1.2.4	COM, IF and POE	C
[2]		tampers	integrity relevant data	permanently stored on the wearable				N
[3]				volatile stored on the wearable				N
[4]				communicated from or to the MP or RDPS		Prevention: [INT-COM] 5.1.4.2	COM, IF and POE	C
[5]		discloses	confidential data	on the wearable	unnecessarily processed	Prevention: [DMIN-DJST] 5.1.6.1		C
[6]				permanently stored on the wearable	during storage	Prevention: [CONF-SSM] 5.1.5.1	POE	C
[7]					after deletion			N
[8]				volatile stored on the wearable	during usage			N
[9]					after usage			N
[10]				communicated from or to the MP or RDPS		Prevention: [CONF-COM] 5.1.5.2	COM, IF and POE	C
[11]		tampers	loss sensitive data	permanently stored on the wearable	during storage			N
[12]			integrity relevant function	on the wearable		Prevention: [INT-SWPCK] 5.1.4.1		N
[13]		impacts the availability of	time sensitive function		by interruption caused by a software update installation	Prevention: [AVAI-SUM-SCHEDULE] 5.1.7.10		C
[14]					by interruption of power supply	Information: [AVAI-TIME-OUTA-NOT] 5.1.7.4 [AVAI-TIME-PREV-NOT] 5.1.7.5 Restoration: [AVAI-TIME-RECO-POW] 5.1.7.1		C

No.	Threat Actor	Threat action	Asset	Threat details		Requirement(s) for mitigation	Relevant attack surface parameter	Risk coverage
[15]					by interruption of network connection	Prevention: [AVAI-TIME-NETW] 5.1.7.2 Information: [AVAI-TIME-OUTA-NOT] 5.1.7.4 [AVAI-TIME-PREV-NOT] 5.1.7.5 Restoration: [AVAI-TIME-RECO-NETW] 5.1.7.3		C
[16]					due to overloading of a resource or connection	Prevention: [AVAI-TIME-NET-PRIO] 5.1.7.6 [AVAI-TIME-RES-PRIO] 5.1.7.7 [AVAI-TIME-DOS-RATE] 5.1.7.9 Information: [AVAI-TIME-OUTA-NOT] 5.1.7.4	IF	C
[17]		exploits an implementation vulnerability to compromise	a product cybersecurity asset			Prevention: [LAS-INVAL] 5.1.9.1 [LAS-INSAN] 5.1.9.2 [NKEV] 5.1.1.1 Information: [NKEV-SUM-NOTIF] 5.1.1.5 [SDC-SUM-NOTIF] 5.1.2.3 Restoration: [NKEV-SUM] 5.1.1.2 [NKEV-SUM-PROVIDE] 5.1.1.3 [NKEV-SUM-AUTO] 5.1.1.4 [SDC-SUM-AUTO] 5.1.2.2		C

- 2062
- 2063
- The columns *Threat Actor*, *Threat Action*, *Asset*, and *Threat Details* describe the threat scenario under consideration.
- 2064
- 2065
- The column *Requirement(s) for mitigation* refers to the mitigations of the risks that arise from the threat scenario.
- 2066
- 2067
- The *Relevant attack surface parameter* column describes which of the attack surface parameters make a difference in mitigation.
- 2068
- 2069
- The *Risk coverage* column describes whether the risk associated with the threat scenario has been reduced to an acceptable residual risk (C) or not (N).
- 2070

2071 **Annex G (informative):**

2072

2073 **Relationship between the present document and ETSI EN**
2074 **303 645/ ETSI TS 103 701**

2075 **This informative annex is intended to provide a mapping between the present document and the content of ETSI**
2076 **TC CYBER's existing work on CIoT devices (ETSI EN 303 645/ ETSI TS 103 701).**

2077

2078

Annex H (informative):

2079

Change history

Version	Information about changes
0.0.1	Early draft
0.0.2	Early draft presented the 2 nd September 2025
0.1.0	Stable draft uploaded the 5 th December 2025
0.2.0	Mature draft presented the 27 th January 2026
0.2.2	Editorial changes
0.2.3	Sent to editHelp
0.2.4	Finalized for HASC assessment

2080

2081

2082

History

Version	Date	Status
V0.2.2	February 2026	Clean-up done by <i>editHelp!</i> E-mail: mailto:edithelp@etsi.org
V0.2.4	March 2026	Version to be shared with HASC

2083

2084