# Draft ETSI EN 304 634 V1.0.0 (2026-07)

**HARMONISED EUROPEAN STANDARD**

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

Reference
DEN/CYBER-EUS-003

Keywords
CRA, cybersecurity, wearable

***ETSI***

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

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

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

# Contents

# Intellectual Property Rights

## Essential patents

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

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

## Trademarks

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

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

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

# Foreword

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

The present document has been prepared under the Commission's Standardisation request M/606 - C(2025)618 [i.3] to provide one voluntary means of conforming to the requirements of EU Regulation No 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (CRA) [i.1].

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

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

# Modal verbs terminology

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

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

# Introduction

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

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

# 1 Scope

The present document specifies technical requirements and corresponding assessment criteria for personal wearable products that have a health monitoring purpose or that are intended for the use by and for children, related to cybersecurity. The products with digital elements in scope, thereafter "personal wearable":

- are specified within the "technical description" of the "category of product" number "19" by the Commission Implementing Regulation (EU) 2025/2392 of 28 November 2025 [i.2] as:
  "Personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745(2)or (EU) 2017/746 of the European Parliament and of the Council do not apply, or personal wearable products that are intended for the use by and for children".
- are only covered within the product context described in clause 4.

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

# 2 References

## 2.1 Normative references

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

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

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

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

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

## 2.2 Informative references

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

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

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

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

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

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

[i.4] prEN 40000-1-1: "Cybersecurity requirements for products with digital elements – Vocabulary" (produced by CEN CENELEC).

NOTE: Version and date to be added upon its publication by CEN CENELEC.

[i.5] prEN 40000-1-3: "Cybersecurity requirements for products with digital elements - Vulnerability Handling" (produced by CEN CENELEC).

NOTE: Version and date to be added upon its publication by CEN CENELEC.

[i.6] ETSI TS 103 732-2 (V1.1.2): "CYBER; Consumer Mobile Device; Part 2: Biometric Authentication Protection Profile Module".

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

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

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

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

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

# 3 Definition of terms, symbols and abbreviations

## 3.1 Terms

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

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

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

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

EXAMPLE: Electric motor, heater, etc.

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

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

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

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

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

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

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

**authorisation policy data:** data asset that contains an authorisation policy

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

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

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

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

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

EXAMPLE: ICMP, DHCP Discovery.

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

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

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

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

**cryptographic mechanism:** security-related procedure using cryptography

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

NOTE 2: The terms "cryptographic primitive", "cryptographic construction", "cryptographic scheme" and "cryptographic protocol" are used consistently with the ECCG Agreed Cryptographic Mechanisms (ACM) catalogue [reference].

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

**cryptographic property:** property provided or supported by a cryptographic mechanism

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

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

**data:** information in digital form

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

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

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

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

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

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

EXAMPLE: Private house or apartment.

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

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

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

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

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

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

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

**guardian:** natural or legal entity with responsibility for the child

NOTE: This includes also parents.

**health data:** data asset that indicates information about physiological functions, health condition or physical fitness of humans

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

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

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

**interface:** shared boundary across which the personal wearable exchanges information

**local communication:** ingoing/outgoing communication which requires physical access to a communication partner's interface or proximity of the communication partner to the personal wearable

EXAMPLE: WLAN interface, Bluetooth® Interface or wired interfaces such as Ethernet or USB.

**location data:** data containing geographical information

**logging mechanism:** personal wearable function that logs events

**logical interface:** interface that does not exist in hardware and can only be used by using another device or a physical interface of a personal wearable

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

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

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

**main product:** personal wearable without the remote data processing solution

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

NOTE: Physical operational environment of smartphones and personal wearables.

**network status data:** data asset that describes MPs' or RDPSs' network connections status

**notification mechanism:** personal wearable function that notifies entities on certain events

**parental control function:** personal wearable's function that enables parents or guardians to control:

- access rights of children on the personal wearable
- sources where children can access external content from, or
- persons that can communicate with the child

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

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

**personal calendar data:** data asset that represents information on a personal calendar

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

**personal notes data:** data asset that represents personal information other than calendar data or contact data

**physical interface:** interface that is part of the hardware of a personal wearable

**physical operational environment:** operational environment describing the physical accessibility

**physical security function:** personal wearable function which provides function output as reaction to function trigger input related to residential physical security

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

EXAMPLE: Internet network or mobile cellular network.

**public data:** data from publicly accessible sources

**public data asset:** data asset derived from public data

**sensor:** device or component able to measure characteristics of its physical environment, generating data input representative of its physical environment

EXAMPLE: Blood pressure sensor, heart rate monitor, accelerometer, etc.

**software update mechanism:** personal wearable function that receives and installs software updates

**strictly local communication:** ingoing/outgoing communication which requires physical presence at a communication partner's interface

EXAMPLE: NFC or other short-range communication.

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

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

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

EXAMPLE: Areas intended for public access.

**user:** human entity using the personal wearable

NOTE: User includes guardian and child.

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

**video data:** data asset that represents video information processed by the personal wearable

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

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

## 3.2 Symbols

Void.

## 3.3 Abbreviations

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

| | |
|---|---|
| ACM | Agreed Cryptographic Mechanisms |
| AES | Advanced Encryption Standard |
| API | Application Programming Interface |
| AUTH.Basic | authentication - protection strength level AUTH.Basic |
| AUTH.Enhanced | authentication - protection strength level AUTH.Enhanced |
| AUTH.Medium | authentication - protection strength level AUTH.Medium |
| AUTH.Strong | authentication - protection strength level AUTH.Strong |
| COM | communication type |
| COM.Adjacent | adjacent communication |
| COM.Local | local communication |
| COM.Public | public communication |
| COM.StrictLocal | strict local communication |
| CONF.COM.Basic | communication of confidential data - protection strength level basic |
| CONF.COM.Enhanced | communication of confidential data - protection strength level enhanced |

| | |
|---|---|
| CONF.COM.Medium | communication of confidential data - protection strength level medium |
| CONF.COM.Strong | communication of confidential data - protection strength level strong |
| CONF.SSM.Basic | confidential persistent storage - strength level basic |
| CONF.SSM.Enhanced | confidential persistent storage - strength level enhanced |
| CONF.SSM.Medium | confidential persistent storage - strength level medium |
| CONF.SSM.Strong | confidential persistent storage - strength level strong |
| CPU | Central Processing Unit |
| CSA | Cybersecurity Act |
| DHCP | Dynamic Host Configuation Protocol |
| DOS | Denial Of Service |
| EUF-CMA | Existential Unforgeability under Chosen Message Attack |
| FAR | False Acceptance Rate |
| FRR | False Rejection Rate |
| GCM | Galois/Counter Mode |
| GPS | Global Positioning System |
| GUI | Graphical User Interface |
| HKDF | HMAC-based Key Derivation Function |
| ICMP | Internet Control Management Protocol |
| IF | interface |
| IF.Any | unspecified interface |
| IF.Human | human interface |
| IF.HumanPhysical | physical human interface |
| IF.Logical | logical interface |
| IF.Machine | machine interface |
| IF.Physical | physical interface |
| IMP | impact class |
| IMP.AVAI.LOSS.High | loss sensitive availability impact class high |
| IMP.AVAI.LOSS.Low | loss sensitive availability impact class low |
| IMP.AVAI.LOSS.Medium | loss sensitive availability impact class medium |
| IMP.AVAI.TIME | time sensitive availability impact class |
| IMP.AVAI.TIME.High | time sensitive availability impact class high |
| IMP.AVAI.TIME.Low | time sensitive availability impact class low |
| IMP.AVAI.TIME.Medium | time sensitive availability impact class medium |
| IMP.CONF | confidentiality impact class |
| IMP.CONF.High | onfidentiality impact class high |
| IMP.CONF.Low | confidentiality impact class low |
| IMP.CONF.Medium | confidentiality impact class medium |
| IMP.FH | impact class for function, whose use can cause harm |
| IMP.FH.CCON | function, which can communicate confidential data impact class |
| IMP.FH.DSN.Low | function, whose use can impact the availability of other devices, services or networks impact class low |
| IMP.FH.High | function, whose use can cause harm impact class high |
| IMP.FH.Low | function, whose use can cause harm impact class low |
| IMP.FH.Medium | function, whose use can cause harm impact class medium |
| IMP.FH.SP | function, whose use can impact the safety or privacy of human entities impact class |
| IMP.FH.SP.High | function, whose use can impact the safety or privacy of human entities impact class high |
| IMP.FH.SP.Low | function, whose use can impact the safety or privacy of human entities impact class low |
| IMP.FH.SP.Medium | function, whose use can impact the safety or privacy of human entities impact class medium |
| IMP.INT | integrity impact class |
| IMP.INT.High | integrity impact class high |
| IMP.INT.Low | integrity impact class low |
| IMP.INT.Medium | integrity impact class medium |
| IND-CCA | Indistinguishability under Chosen-Ciphertext Attack |
| IND-CCA2 | Indistinguishability under adaptive Chosen-Plaintext Attack |
| IND-CPA | Indistinguishability under Chosen-Plaintext Attack |
| INT.COM.Basic | communication of integrity relevant data - protection strength level basic |
| INT.COM.Enhanced | communication of integrity relevant data - protection strength level enhanced |
| INT.COM.Medium | communication of integrity relevant data - protection strength level medium |
| INT.SSM.Basic | integrity protecting persistent storage - strength level basic |
| INT.SSM.Enhanced | integrity protecting persistent storage - strength level enhanced |
| INT.SSM.Medium | integrity protecting persistent storage - strength level medium |

| | |
|---|---|
| INT.SSM.Strong | integrity protecting persistent storage - strength level strong |
| INT.SW.VER.Basic | software package integrity verification - strength level basic |
| INT.SW.VER.Enhanced | software package integrity verification - strength level enhanced |
| INT.SW.VER.Medium | software package integrity verification - strength level medium |
| IP | Internet Protocol |
| LED | Light-Emitting Diode |
| LOE | logical operational environment |
| MFA | Multi Factor Authentication |
| MP | Main Product |
| N/A | not applicable |
| NFC | Near Field Communication |
| PIN | Personal Identification Number |
| PitM | Person-in-the-Middle |
| POE | physical operational environment |
| POE.Any | unspecified physical operational environment |
| POE.FullyControlled | fully controlled physical operational environment |
| POE.Mobile | mobile operational environment |
| POE.MobileControlled | controlled mobile operational environment |
| POE.PartiallyControlled | partially controlled physical operational environment |
| RDPS | Remote Data Processing Solution |
| ROM | Read Only Memory |
| SBOM | Software Bill Of Material |
| SFA | Single Factor Authentication |
| SOTA | State Of The Art |
| SUF-CMA | Strong existential Unforgeability under Chosen Message Attack |
| TLS | Transport Layer Security |
| UPnP | Universal Plug and Play |
| USB | Universal Serial Bus |
| VPN | Virtual Private Network |
| WLAN | Wireless Local Area Network |
| XTS | XEX-based Tweaked-codebook mode with Ciphertext Stealing |

# 4 Product context

## 4.0 Introduction

### 4.0.1 General

Two kinds of products are considered in the present document: personal wearable that have a health monitoring purpose and personal wearable that are intended for the use by and for children. Both hardware and software products may fall in this category, but most products include a combination of hardware (including sensors and some processing capabilities) and hosted software.

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

- smart watches;
- fitness bands;
- smart glasses;
- heart rate monitor;
- smart socks;
- headbands;
- biomechanical shoe insoles;

- skin patches.

Personal wearable that are intended for the use by and for children can be divided in two categories depending to the age of the child. There is a clear separation between the personal wearables for babies under 2-year-old, for which the monitoring is much more extensive but without the need of the baby to manage the device, and the preadolescent children where GPS tracking and Parental Control are key functionalities. The present document handles this separation introducing specific data and functions assets.

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

- smartwatches with GPS tracking and parental control

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

- baby monitoring system including:
  - baby smart socks
  - sensor bracelet for breathing monitoring
  - Smart wearable breast pumps
  - Smart pacifiers - with temperature check-ups and GPS tracker

### 4.0.2 Personal wearable that have a health monitoring purpose

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

1) the health monitoring which means the continuous collection, analysis and visualisation of the analysed physiological and health-related data (e.g. heart rate, blood oxygen levels, stress level or other vital signs) using sensors included in the personal wearable;

2) the activity tracking which means collecting and analysing (automatically or on demand) data like the number of steps done, distance gone, exertion, intensity and burned calories during activities like walking, jogging, bicycling, swimming, dancing, etc.

### 4.0.3 Personal wearable that are intended for the use by and for children

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

1) the health monitoring which means the continuous collection, analysis and visualisation 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 personal wearable.

2) The location tracking to monitor the child position.

3) Parental control to allow children parents to control the child activities on the personal wearables.

## 4.1 Product functions

### 4.1.0 Introduction

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

### 4.1.1 Health monitoring functionalities (essential functionalities)

It includes the physiological data acquisition using sensors, physiological data signal processing, analysis and visualisation. Examples of sensors include light source and photodetector, accelerometers, gyroscopes, temperature sensor, skin response sensor, pulse oximeter sensor ($SP0_2$), 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 visualisation 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 personal 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.

### 4.1.2 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;
- localisation which determines the precise location;
- geofencing which creates virtual boundaries.
- the location tracking to monitor the children position.

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

### 4.1.3 Parental Control (essential functionalities)

It includes the functionalities allowing the parents or the guardians to put limitations in the usage of the personal wearable by the children. The functionalities may include:

- configuration of the children permission on the personal wearable;
- configuration of the geofencing parameters;
- possibility to access remotely to the audio and/or video capabilities of the personal wearable;
- possibility to track the children personal wearable position

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

### 4.1.4 Notification functionalities (essential functionalities)

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

Examples of notification functionalities include:

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

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

### 4.1.5 Input commands from user or other connected devices (supporting functionalities)

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

### 4.1.6 Data monitoring and storage (supporting functionalities)

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

### 4.1.7 General functionalities (supporting functionalities)

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

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

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

### 4.1.8 Summary of the personal wearable functions

The present document addresses the following personal wearable essential functionalities:

- health monitoring functionalities

- health monitoring functionalities (for babies care use)
- activity monitoring functionalities
- positioning functionalities
- location sharing functionalities
- emergency location functionalities
- location sharing functionalities (for children use)
- geofencing (for children use)
- parental control functionalities (for children use)
- notification functionalities
- audio functionalities
- video functionalities
- functionalities which can communicate personal wearable data assets

The present document addresses the following personal wearable supporting functionalities:

- logging mechanism
- input sanitisation mechanism
- input validation mechanism
- configuration functionalities
- software update mechanism
- access control mechanism
- authentication mechanism
- factory reset function
- integrity protecting communication mechanism
- confidentiality protecting communication mechanism
- integrity protecting secure storage mechanism
- confidentiality protecting secure storage mechanism
- deletion mechanism
- software package verification mechanism
- bootloader functionalities

### 4.1.9 Data assets

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

- health data;
- activity data;
- input data from sensors;

- location data, including device location data;
- location data (for children use), including device location data;
- audio data;
- video data;
- audio (for children use);
- video (for children use);
- network status data;
- access control policy data;
- social interactive data;
- social interactive data (for children use);
- confidential data;
- personal calendar data;
- personal contact data;
- personal notes data.

## 4.2 Product Architecture

### 4.2.0 Introduction

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

### 4.2.1 Personal wearable that have a health monitoring purpose architecture

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

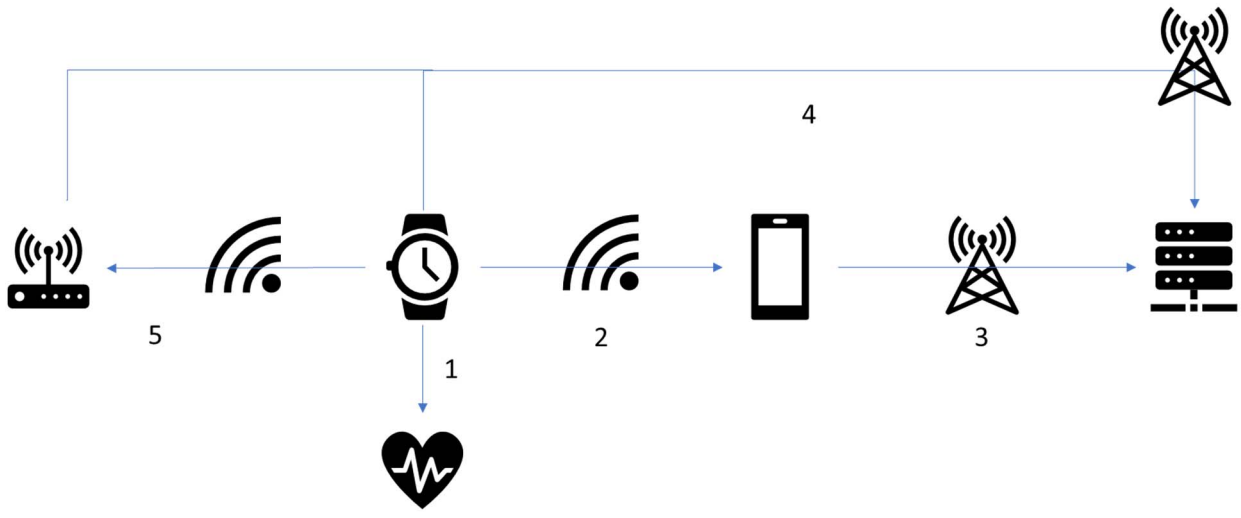


**Figure 1: Health monitoring personal wearable architecture**

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

2) The personal 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 personal 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 personal 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.

3) The mobile application associated to the personal wearable device may be connected to a remote service hosted in the cloud. The radio link is typically 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 personal wearable device that will be delivered through the link described in point 2.

NOTE 1: The cloud service may constitute a remote data processing solution.

4) The personal 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 personal wearable device transfers to the cloud application processed data, activity report, health report and a backup of all the personal wearable device data in order to be able to move them on another personal wearable device if the user decide to change it. The server to which the personal wearable device is connected can be also provide software updates.

NOTE 2: The cloud service may be considered a remote data processing solution.

5) The personal 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.

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

- The main product (hardware and software)
- The mobile application (optional)
- The cloud service acting as remote data processing service (optional)
- The gateway (optional)

### 4.2.2 Personal wearable that are intended for the use by and for children architecture

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

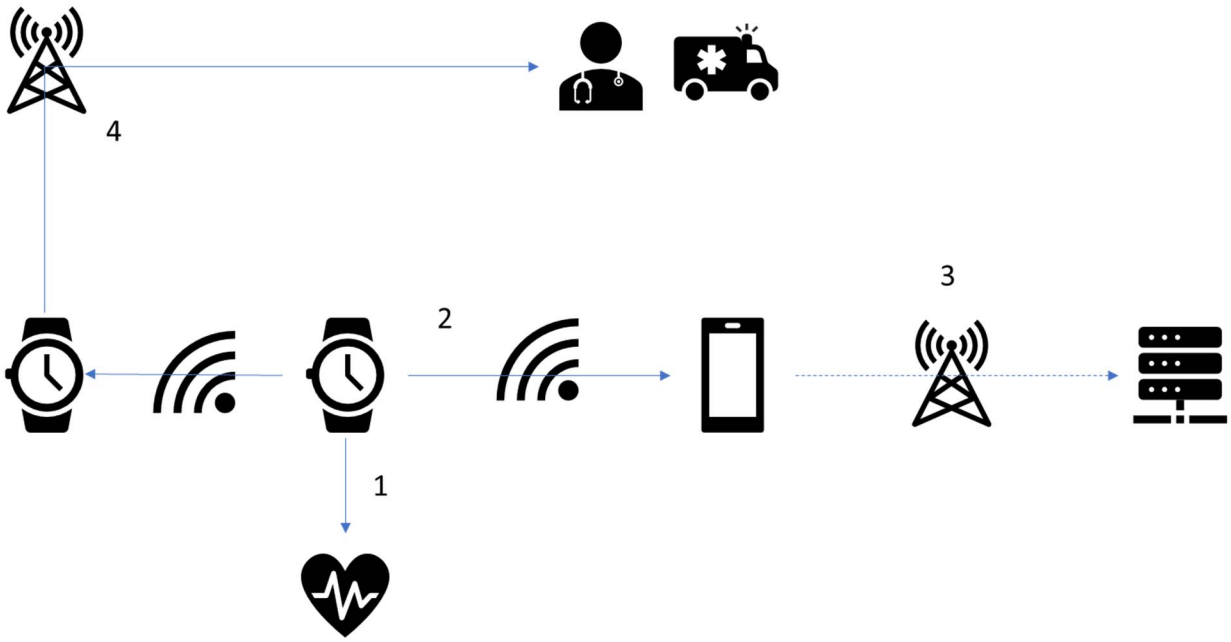


**Figure 2: Health monitoring personal wearable architecture**

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

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

3) The mobile application associated to the personal wearable device may be connected to a remote cloud service. The radio link may be Wi-Fi or cellular. Through this link the mobile application transfers to the cloud service 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 cloud service to which the mobile application is connected may also provide software updates for the personal wearable device that will be delivered through the link described in point 2.

NOTE 1: the cloud service may be considered a remote data processing solution.

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

NOTE 2: the emergency services infrastructure may be considered a remote data processing solution.

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

1) The main product (hardware and software)

2) The mobile application (optional)

3) The cloud service acting as remote data processing service (optional)

4) The emergency services infrastructure acting as remote data processing solution (optional)

5) The guardian's personal wearable (optional; it may be an ancillary device not provided with the main product)

## 4.3 Operational Environment

### 4.3.1 General description

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

### 4.3.2 Physical operational environment

The physical environment of the personal wearable devices may include all typical consumer electronic physical environments, including homes, offices, wellness centres, but also outdoor spaces such as rural areas, city streets, sport stadiums.

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

- fully controlled physical operational environment - POE.FullyControlled
- partially controlled physical operational environment - POE.PartiallyControlled
- mobile operational environment - POE.Mobile
- controlled mobile operational environment - POE.MobileControlled

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

- fully controlled physical operational environment - POE.FullyControlled
- partially controlled physical operational environment - POE.PartiallyControlled
- mobile operational environment - POE.Mobile

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

- fully controlled physical operational environment - POE.FullyControlled.

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

### 4.3.3 Logical operational environment

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

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

### 4.3.4 Connectivity aspects

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

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

- logical interface - IF.Logical
- physical interface - IF.Physical

## 4.4 Distribution of Security Functions

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

"The personal wearable shall […] use [some expression related to security functions]" means:

- the personal wearable itself provides those security functions which are always used, or
- other products with digital elements in the personal wearable's context provide those security functions which are always used by the personal wearable.

"The personal wearable shall […] support [some expression related to security functions]" means:

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

"The personal wearable shall […] provide [some expression related to security functions]" means that the personal wearable itself provides those security functions.

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

## 4.5 Users

### 4.5.1 End-Users

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

The present document addresses personal wearables having the following using entities:

- user
- child
- guardian

### 4.5.2 Manufacturers

Manufacturers deliver the product to market which may be coming together with a manufacturer mobile application and remote data process services. Guidelines are provided to the end-user for setting-up the personal wearable and connecting the personal wearable to the mobile phone or generally to the internet using state-of-the art security methods. Manufacturers are pushing software updates to the personal wearable device and keep the software updated.

The present document addresses personal wearables having the following using entities:

- manufacturer

## 4.6 Use cases

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

In order to classify use cases and to define security profiles the following use case profiles are defined. Those definitions make use of impact classes of essential functionalities. The essential functionalities covered by the present document are provided in clause 4.1.7, their impact classes are provided in Annex D.

# 5 Technical requirements for personal wearables

## 5.1 Introduction - Applicability of the requirements

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

Not all requirements are universally applicable: the applicability of requirements may be based on use cases or specific capabilities of the product.

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

## 5.2 Appropriate level of cybersecurity

### 5.2.0 Appropriate level of cybersecurity introduction

This clause addresses the requirements in the CRA [i.1] Annex I Part I (1).

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

The personal wearable shall detect and notify a user when security functions that are supposed to be used or supported by the personal wearable are not available.

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

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

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

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

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

- clearly distinguish security-related configuration options visually from other configuration options; and

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

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

The personal wearable shall support data transfer mechanisms for all loss sensitive data permanently stored at the personal wearable.

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

The personal wearable shall support automatic data transfer mechanisms for all loss sensitive data of impact class IMP.AVAI.LOSS.Medium or higher permanently stored at the personal wearable.

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

Where the personal wearable is intended to be installed or maintained by a consumer for private usage, the personal wearable shall support data export mechanisms for all loss sensitive data of impact class IMP.AVAI.LOSS.Medium or higher permanently stored at the personal wearable such that the user can export the data stored at an architectural component:

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

## 5.3 No known exploitable vulnerabilities

### 5.3.0 No known exploitable vulnerabilities introduction

This clause addresses the requirements in the CRA [i.1] Annex I Part I (2) (a).

### 5.3.1 [NKEV-MKAV] No known exploitable vulnerabilities

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

NOTE 1: The known exploitable vulnerabilities that occur after making the personal wearable available on the market are subject to the vulnerability handling in CEN/CLC JT013090:2026 (prEN 40000-1-3 [i.5]).

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

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

The personal wearable's architectural components shall:

- request information on the availability of security update packages; and
- notify users when security update packages are available; and
- (if authorised by users) request and install available security update packages

before or during first use.

NOTE: User authorisation for automated security update is described in clauses 5.5.4 and 5.5.5.

## 5.4 Secure by default configuration

### 5.4.0 Secure by default configuration introduction

This clause addresses the requirements in the CRA [i.1], Annex I Part I (2) (b).

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

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

- the authentication mechanisms strengths specified in clause E.1.1; and
- the minimal authentication mechanisms' strength determined by Table 3;

except for connection functions.

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

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

Where:

- The personal wearable has the capability to connect to a public network; and
- No time sensitive function with IMP.AVAI.TIME.High is provided by an architectural component,

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

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

NOTE 2: The user can decide to turn off the automated security update mechanism and manually perform the update when is more suitable for him. For example, the user does not want to update the personal wearable during a sport session where health and activity data are monitored or when the software update can interfere with parental control functionalities.

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

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

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

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

The personal wearable shall provide a factory reset mechanism that allows a user to restore the default state, including the deletion of all user data, installed applications, and configurations deviating from the default state, except deviations due to security.

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

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

### 5.4.5 [SDC-PARCONT] Default configuration for parental control

Where the personal wearable supports the parental control functions, the personal wearable shall by default be configured to:

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

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

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

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

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

The personal wearable shall by default be configured to use:

- a logging mechanism; or
- where the architectural component does not support public communication or where the personal wearable main product has constrained memory storage capabilities, a data transfer mechanism;

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

### 5.4.7 [CRY-SOTA] State-of-the-art cryptography

The personal wearable shall by default only use cryptographic mechanisms for cryptographic functions as described in Annex K.

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

The personal wearable shall only provide preinstalled confidential cryptographic keys of key sizes that are:

- listed in Annex K; or
- provide a minimum security strength of 112 bits.

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

The personal wearable shall by default only generate confidential cryptographic keys of key sizes that are:

- listed in Annex K; or
- provide a minimum security strength of 112 bits.

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

The personal wearable shall only provide preinstalled passwords:

- that meet the minimal recommended password complexity C_{PW,min} determined by the corresponding authentication mechanisms' usage according to Table 3; and
- that are either:
  - individual per personal wearable and not derivable via publicly available information; or
  - random per personal wearable.

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

The personal wearable shall by default only generate passwords of minimal recommended password complexity C_{PW,min} determined by the corresponding authentication mechanisms' usage according to Table 3 and that are random.

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

The personal wearable shall only use user chosen passwords of minimal recommended password complexity C_{PW,min} determined by the corresponding authentication mechanisms' usage according to Table 3, except for user chosen passwords where the user explicitly confirms their usage after a warning by the personal wearable.

## 5.5 Security updates

### 5.5.0 Security updates introduction

This clause addresses the requirements in the CRA [i.1], Annex I Part I (2) (c).

### 5.5.1 [SU-SUPPORT] Software update mechanism

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

NOTE 1: An application distribution platform installed on a mobile device provides updates for mobile applications that are part of the personal wearable. In some cases, where the application to be updated is part of the personal wearable's core software, the core software update mechanism provides also the application updates.

NOTE 2: part of the personal wearable's software can be immutable due to its technology (e.g. software installed in a ROM).

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

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

NOTE 1: A mobile application typically does not need to provide an update mechanism.

NOTE 2: part of the personal wearable's software can be immutable due to its technology (e.g. software installed in a ROM).

### 5.5.3 [SU-AUTO] Automated security updates

Where:

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

the personal wearable shall support the automated security update of its software within an appropriate time frame.

NOTE 1: Automatic installation of security updates could create an unacceptable risk to essential function availability or safety in situations where installation could interrupt availability relevant essential functions or create safety risks in foreseeable emergency use (e.g. delaying an emergency call, preventing parents to localise their children, or preventing timely alarm related to children health).

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

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

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

Where the personal wearable provides mechanisms for automated update of personal wearable's software operated by users, the personal wearable shall provide a clear and easy-to-use option for users to disable those mechanisms.

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

Where the personal wearable provides mechanisms for automated update of personal wearable's software operated by users, the personal wearable shall provide an option for users to temporary postpone the installation of updates.

### 5.5.6 [SU-NOTIF] Update notifications

Where the personal wearable has the capability to connect to a public network, the personal wearable shall support the automated notification of its users, when updates of its software are available.

## 5.6 Authentication and access control

### 5.6.0 Authentication and access control introduction

This clause addresses the requirements in the CRA [i.1], Annex I Part I (2) (d).

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

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

**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 |
| | COM.Adjacent via IF.Any | | Applicable | Applicable | Applicable |
| | COM.Public via IF.Any | | Applicable | Applicable | Applicable |

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

- factory reset function
- functions configured by parental control function

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

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

- the authentication mechanisms strengths are specified in clause E.1.1; and
- the minimal required authentication strength is determined by Table 3;

except for connection functions.

**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[*] |
| | | POE.PartiallyControlled | N/A | AUTH.Basic[*] | AUTH.Medium[*] |
| | | POE.Mobile | AUTH.Basic[*] | AUTH.Medium[*] | AUTH.Enhanced[*] |
| | | POE.Controlled.Mobile | N/A | AUTH.Basic[*] | AUTH.Medium[*] |
| | 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[*] | AUTH.Medium[*] |
| | 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 |

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

- factory reset function
- functions configured by parental control function

### 5.6.3 [AUTHZ-LP] Least privilege in authorisation policies

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

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

EXAMPLE 1: A personal wearable typically has only one user, therefore, all permissions are granted to that user.

EXAMPLE 2: A personal wearable with parental control functions has more than one user, therefore, different permissions are granted to different roles (i.e. child, guardian).

### 5.6.4 [AUTHZ-R] Revocability of granted permissions

The personal wearable shall support the revocation of any permission granted by an authorised entity.

EXAMPLE: An administrative user can revoke permissions granted to another user.

### 5.6.5 [PARCONT] Support of parental control

Where the personal wearable is used for children, the personal wearable shall support parental control functions, covering the parents' or guardians' control of:

- access rights on the personal wearable of children;
- personal wearable position;

- where the personal wearable allows children to access external content, the sources where children are allowed to access external content from; and
- where the personal wearable allows children to communicate with other persons, the persons that are allowed to communicate with children.

### 5.6.6 [AUTHZ-PC] Authorisation policies for parental control

If the personal wearable supports the parental control, the personal wearable shall use an authorisation policy that:

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

## 5.7 Confidentiality protection

### 5.7.0 Confidentiality protection introduction

This clause addresses the requirements in the CRA [i.1], Annex I Part I (2) (e).

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

The personal wearable shall use confidentiality protecting secure storage mechanisms for persistently stored confidential data, where the mechanisms' strength is specified in clause E.3.1 and the minimal required mechanisms' strength are determined by Table 7.

NOTE 1: The requirement applies only to personal wearable's storage means; external storage means such as memory card are out of the scope.

NOTE 2: Typically, encryption/decryption keys for storage encryption are stored such that they cannot be extracted. Corresponding protection measures are subject to confidential persistent storage - strength level strong.

**Table 7: 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[*] | CONF.SSM.Medium |
| | POE.Mobile | CONF.SSM.Basic[*] | CONF.SSM.Medium | CONF.SSM.Enhanced |
| | POE.MobileControlled | N/A | CONF.SSM.Basic[*] | CONF.SSM.Medium |

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

- which is persistently stored on non-removable storage.

### 5.7.2 [CONF-COM] Communication of confidential data

The personal wearable shall use confidentiality protecting communication mechanisms to protect the confidentiality of communicated confidential data, where the corresponding confidentiality protection measures strengths are specified in clause E.3.2 and the minimal required confidentiality protection measures' strength are determined by Table 8.

NOTE: The personal wearable can communicate data with other devices or services and between architectural components, e.g. between a personal wearable's mobile application and its RDPS.

**Table 8: Assignment of protection mechanisms strength level for the confidentiality of communicated data**

| | | | confidential data impact class | | |
|---|---|---|---|---|---|
| | | | **IMP.CONF.Low** | **IMP.CONF.Medium** | **IMP.CONF.High** |
| **Attack Surface determined by COM, IF and POE of RDPS or MP that communicates confidential data** | COM.StrictLocal via IF.Human | POE.Any | N/A | N/A | CONF.COM.Basic[*] |
| | 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.Mobie | 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[*] |

For protection measures labelled with [*], it is not required that the personal wearable uses confidentiality protecting communication mechanisms for confidential data:

- which is used as connection data.

### 5.7.3 [CONF-MON-HW] Indication of active capture of audio or video data

Where the Personal Wearable continuously captures audio and/or video data the Personal Wearable shall use a visual or auditory indicator, to indicate, in real time, when audio and/or video data is captured.

EXAMPLE: Smart Glasses recoding audio and video data which gives a visual or audio indication of the recording action.

## 5.8 Integrity protection

### 5.8.0 Integrity protection introduction

This clause addresses the requirements in the CRA [i.1], Annex I Part I (2) (f).

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

The personal wearable shall use integrity protecting secure storage mechanisms for persistently stored integrity relevant data, where the mechanisms' strength is specified in clause E.2.1 and the minimal required mechanisms strength are determined by Table 4.

**Table 4: Assignment for integrity protecting secure storage mechanisms**

| | | Integrity impact class for persistently stored integrity relevant data | | |
|---|---|---|---|---|
| | | **IMP.INT.Low** | **IMP.INT.Medium** | **IMP.INT.High** |
| **Attack Surface determined by POE of the architectural component that persistently stores integrity relevant data** | POE.FullyControlled | N/A | N/A | N/A |
| | POE.PartiallyControlled | N/A | INT.SSM.Basic[*] | INT.SSM.Medium |
| | POE.Mobile | INT.SSM.Basic[*] | INT.SSM.Medium | INT.SSM.Enhanced |

For protection measures labelled with [*], it is not required that the personal wearable uses integrity protecting persistent storage for integrity relevant data:

- which is persistently stored on non-removable storage.

## 5.8.2 [INT-SWPCK] Software package verification

The personal wearable shall use software package verification mechanisms to verify the integrity and authenticity of software packages prior to installation where the software package verification mechanism's strength levels are specified in clause E.2.2 and where the minimal software package verification mechanism's strength is determined by Table 5.

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

**Table 5: Assignment of the software package verification mechanism's strength levels for the 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 |

## 5.8.3 [INT-COM] Communication of integrity relevant data

The personal wearable shall use integrity protecting communication mechanisms to protect the integrity of communicated integrity relevant data, where the corresponding integrity protection measures strengths are specified in clause E.2.3 and the minimal required integrity protection measures' strength are determined by Table 6.

**Table 6: Assignment of protection mechanisms strength level for the integrity protection of outgoing data and for the integrity verification of incoming data**

| | | | Integrity relevant data impact class | | |
|---|---|---|---|---|---|
| | | | **IMP.INT.Low** | **IMP.INT.Medium** | **IMP.INT.High** |
| **Attack Surface determined by COM, IF and POE of 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[*] |

For protection measures labelled with [*], it is not required that the personal wearable uses integrity protecting communication mechanisms of strength higher than INT.COM.Basic to protect the integrity of communicated integrity relevant data:

- which is used as connection data.

## 5.9 Data minimisation

### 5.9.0 Data minimisation introduction

This clause addresses the requirements in the CRA [i.1], Annex I Part I (2) (g).

### 5.9.1 [DMIN-DJST] Documented justification of processed data

The personal wearable shall only process data which are adequate, relevant and limited to its intended purpose.

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

## 5.10 Availability protection

### 5.10.0 Availability protection introduction

This clause addresses the requirements in the CRA [i.1], Annex I Part I (2) (h).

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

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

### 5.10.2 [AVAI-TIME-NETW] Local operation

Where network connectivity is not necessary for a time sensitive function to operate, the personal wearable shall ensure the operability of this function in the case of a loss of network access.

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

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

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

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

EXAMPLE: A personal wearable loses connection to the local network as the network is temporarily unavailable. After recognising the restored network, the personal wearable reconnects after a randomised delay to reconnect cleanly.

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

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

EXAMPLE: A cloud RDPS recognizes a non-availability of its MP and sends a notification to the user or a mobile application indicates that the MP is not connected.

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

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

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

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

### 5.10.6 [AVAI-TIME-PREV-PRIO] Network prioritisation

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

- such that these functions are prioritised according to their IMP.AVAI.TIME; or
- such that functions are prioritised according to user decisions or configuration.

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

Where:

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

the personal wearable shall use a mechanism to prioritize the use of power in the case of a low power condition:

- such that these functions are prioritised according to their IMP.AVAI.TIME; or
- such that functions are prioritised according to user decisions or configuration.

### 5.10.8 [AVAI-UPD-SCHEDULE] Scheduling of updates

Where:

- the personal wearable has the capability to connect to a public network; and
- at least one time sensitive function with IMP.AVAI.TIME.Medium or higher is provided by the personal wearable;

the personal wearable shall support the scheduling of the application of updates that can impact the availability of these functions with IMP.AVAI.TIME.Medium or higher.

## 5.11 Non-interference

This clause addresses the requirements in the CRA [i.1], Annex I Part I (2) (i).

Not applicable see Annex A.

## 5.12 Attack surface minimisation

### 5.12.0 Attack surface minimisation introduction

This clause addresses the requirements in the CRA [i.1], Annex I Part I (2) (j).

### 5.12.1 [LAS-INVAL] Validation of external data input

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

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

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

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

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

### 5.12.2 [LAS-INSAN] Sanitisation of external data input

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

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

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

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

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

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

### 5.12.5 [LAS-SBOOT] Secure boot

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

NOTE 1: The requirement corresponds to the verified boot capability in ETSI EN 304 623 [i.7].

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

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

## 5.13 Exploit mitigation

### 5.13.0 Exploit mitigation introduction

This clause addresses the requirements in the CRA [i.1], Annex I Part I (2) (k).

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

The personal wearable's architectural components shall use mechanisms to ensure that privileges to access architectural components':

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

for processes running on the same hardware, are only assigned where necessary for the personal wearable's intended purpose.

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

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

The personal wearable's architectural components shall use mechanisms to ensure that privileges to access processes implementing architectural components':

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

for processes running on the same hardware, are only assigned where necessary for the personal wearable's intended purpose.

## 5.14 Monitoring

### 5.14.0 Monitoring introduction

This clause addresses the requirements in the CRA [i.1], Annex I Part I (2) (l).

### 5.14.1 [MON-LOW] Events to log for low risk personal wearable

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

- abnormal shutdowns;
- errors of the core software.

### 5.14.2 [MON-MEDIUM] Events to log for medium risk personal wearable

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

- unsuccessful authentication attempt;
- abnormal shutdowns;
- errors of the core software.

### 5.14.3 [MON-HIGH] Events to log for high risk personal wearable

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

- unsuccessful authentication attempt;
- abnormal shutdowns;
- errors of the core software;
- every unsuccessful attempt to gain additional privileges that are critical to the protection of the personal wearable;

### 5.14.4 [MON-HANDLE] Handling of events

The personal wearable shall support:

- a logging mechanism; or
- where the architectural component does not support public communication or where the personal wearable main product has constrained memory storage capabilities, a data transfer mechanism;

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

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

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

### 5.14.5 [LOG-TIME] Timestamps for logs

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

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

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

### 5.14.7 [LOG-STORE-MEDIUM] Logfile persistence for medium risk personal wearable

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

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

before deletion or rotation of logging data.

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

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

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

### 5.14.8 [LOG-STORE-HIGH] Logfile persistence for high risk personal wearable

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

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

before deletion or rotation of logging data.

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

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

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

### 5.14.9 [LOG-CONFIG] Configuration of logging mechanisms

Where the personal wearable uses logging mechanisms the personal wearable shall provide a clear and easy to use option for users to disable those mechanisms unless the disabling of the logging mechanism will introduce security issues.

## 5.15 Factory reset and data portability

### 5.15.0 Factory reset and data portability introduction

This clause addresses the requirements in the CRA [i.1], Annex I Part I (2) (m).

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

The personal wearable shall provide at least one deletion mechanism that:

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

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

# 6 Assessment criteria for compliance with technical requirements

## 6.1 Introduction to the assessment and compliance criteria

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

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

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

- **Assessment reference:** Refers to the identifier of the concerned technical requirement.
- **Assessment objective:** Defines the security property or capability that shall be verified, ensuring that the assessment remains focused on the intent of the requirement.
- **Assessment preparation:** Describes the environment, setup, and preconditions required before executing the test with a view to guaranteeing consistent evaluation results. It includes the following elements as applicable:
  - Test environment: Describe the hardware, software, and network setup used for the assessment, including versions, topology, and any relevant dependencies.
  - Preconditions: Specify any configurations, credentials, or operational states that should be established before the test (e.g. product initialized, certificates loaded, user roles created).
  - Required tools: Identify the tools or software necessary to perform the assessment (e.g. vulnerability scanners, protocol fuzzers, traffic analysers, static code analysers, cryptographic test suites).
  - Required information/documentation for the assessment: Specify all information that is necessary to perform the assessment.
  - Reference any vendor-provided setup guides, configuration instructions, or operational manuals, as well as any relevant standards or technical notes, that define how the product shall be configured or operated for the assessment.
- **Assessment activities:** Provides execution steps to be performed such that the same assessment verdict would be reached when repeating these steps now or at a later point in time. Assessment activities may include, as applicable:
  - Review information/documentation for the assessment to confirm that the described implementation matches the requirement (e.g. verify that the security architecture document specifies TLS 1.2 or higher for all external interfaces, or that the password policy aligns with the defined threshold).
  - Perform security functional tests to verify the completeness and correctness of the information/documentation for the assessment.

- Perform security functional or penetration tests to verify that implemented controls are correctly implemented e.g. to prevent unauthorized access or data modification (e.g. via attempting to log in with invalid credentials to test lockout enforcement or trying to modify protected configuration files without administrative privileges).
- Analyse code or binaries to identify potential security weaknesses or misconfigurations (e.g. perform static analysis to detect hardcoded credentials or use dynamic analysis tools to identify buffer overflow or injection vulnerabilities).
- Inspect configurations to ensure that required security parameters are correctly applied (e.g. check that weak cipher suites are disabled, two-factor authentication is enabled, and least-privilege access controls are configured in the system).
- Observe runtime behaviour to confirm that protections such as encryption, authentication, and integrity verification operate as intended (e.g. monitor network traffic to ensure data in transit is encrypted or observe system logs to verify successful validation of digital signatures during startup).

- **Assessment verdict:** Defines the pass/fail criteria.
  - **Pass:** The assessment is considered passed if the product demonstrably fulfils the requirement and meets the defined security thresholds. Examples of such thresholds include:
    - Minimum cryptographic strength (e.g. AES-128 or higher);
    - Password policy limits (e.g. minimum of 12 characters);
    - Login protection mechanisms (e.g. account lockout after five consecutive failed attempts);
    - Resistance to a specified attack potential (e.g. equivalent to CSA High/AVA_VAN.3 or higher).
  - **Fail:** The assessment is considered failed if the requirement is not fulfilled, or if the defined security thresholds are not achieved (e.g. insufficient key length, missing authentication enforcement, or inadequate resistance to the required attack potential).
- **Assessment evidence:** Defines the artefacts and documentation collected to demonstrate that the requirement has been assessed and fulfilled. The evidence shall be sufficient to enable independent verification of the assessment results and to demonstrate compliance with the relevant CRA essential requirements. The supporting evidence includes, where applicable:
  - Test or assessment reports showing the steps performed and results obtained;
  - Logs, configuration files, or audit traces demonstrating the implementation of the requirement;
  - Screenshots, captures, or console outputs confirming the correct execution or protection behaviour;
  - Relevant vendor or design documentation describing the applied security measures.

## 6.2 Appropriate level of cybersecurity

### 6.2.1 Assessment criteria for [USERNOT-NOSECFUC]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [USERNOT-NOSECFUC]

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- a list of personal wearable's architectural components;

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

**Assessment activities:**

- The personal wearable's conformity to [USERNOT-NOSECFUC] shall be validated based on the documentation.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the documentation indicates the personal wearable's conformity to [USERNOT-NOSECFUC]; and

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- records of the validation of the documentation.

### 6.2.2 Assessment criteria for [USERNOT-SECREL]

**Assessment objective:**

The assessment covers:

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

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

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

The following test setups shall be prepared:

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

**Assessment activities:**

The personal wearable's conformity to [USERNOT-SECREL] shall be validated based on the documentation. The correctness of the implementation shall be verified by inspecting for each used user notification mechanism for security-related notifications whether:

- one security-related notification is clear, understandable, intelligible, legible and can be easily understood by users; and

- (where other notifications are possible), the representation of security-related notifications is clearly distinguished from other notifications.

**Assignment of verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

### 6.2.3 Assessment criteria for [GUI-SECCONF]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [GUI-SECCONF];
- a functional sufficiency assessment concerning [GUI-SECCONF] for each personal wearable's GUI for security-related configuration function.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

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

The following test setups shall be prepared:

- a test setup for accessing each personal wearable's GUI for security-related configuration function.

**Assessment activities:**

The personal wearable's conformity to [GUI-SECCONF] shall be validated based on the documentation. The correctness of the implementation shall be verified by inspecting for each personal wearable's GUI for security-related configuration function whether:

- the visual representation of security-related configuration options is clearly visual distinguished from other configuration options; and
- the consequences of one security-related configuration option are communicated in a clear, understandable, intelligible, legible manner and can be easily understood by users; and
- the change of one security-related configuration is clearly highlighted visually.

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- records of the validation of the documentation

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

### 6.2.4 Assessment criteria for [BACKUP-TRANS]

**Assessment objective:**

The assessment covers:

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

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

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

The following test setups shall be prepared:

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

**Assessment activities:**

- The personal wearable's conformity to [BACKUP-TRANS] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by:
  - an inspection of the personal wearable's physical human interfaces for persistently stored loss sensitive data;

- a scan of the personal wearable's logical interfaces for persistently stored loss sensitive data.

- For each documented data transfer mechanism, its correct implementation shall be verified triggering the transfer and receiving loss sensitive data.

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

### 6.2.5 Assessment criteria for [BACKUP-AUTOTRANS]

**Assessment objective:**

The assessment covers:

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

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

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

The following test setups shall be prepared:

- for each architectural component, a test setup based on a sample personal wearable in default configuration for identifying:
  - loss sensitive data persistently stored at the architectural component; and

- for each documented automatic data transfer mechanism, a test setup to generate and automatically receive loss sensitive data.

**Assessment activities:**

- The personal wearable's conformity to [BACKUP-AUTOTRANS] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by:
  - an inspection of the personal wearable's physical human interfaces for persistently stored loss sensitive data of impact class [IMP.AVAI.LOSS.Medium] or higher;
  - a scan of the personal wearable's logical interfaces for persistently stored loss sensitive data of impact class [IMP.AVAI.LOSS.Medium] or higher.
- For each documented automatic data transfer mechanism, its correct implementation shall be verified generating and automatically receiving loss sensitive data.

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

### 6.2.6 Assessment criteria for [BACKUP-EXPORT]

**Assessment objective:**

The assessment covers:

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

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- a list of personal wearable's architectural components;

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

The following test setups shall be prepared:

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

**Assessment activities:**

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

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

descriptions of the performed tests and records of performed tests to verify the correct implementation of each data export mechanism.

## 6.3 No known exploitable vulnerabilities

### 6.3.1 Assessment criteria for [NKEV-MKAV]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [NKEV-MKAV], where potential known exploitable vulnerabilities are identified either:
  - based on an SBOM; or
  - based on a vulnerability scanner applied to the default configuration of the personal wearable required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- a remediation plan for known exploitable vulnerabilities
- (if the assessment is based on a SBOM and the SBOM is transitive) the SBOM of the personal wearable.

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

- the personal wearable shall be set up in default configuration;
- a vulnerability scanner for the personal wearable shall be set up.

**Assessment activities:**

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

**Assessment verdict:**

The verdict PASS shall be assigned when:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

### 6.3.2 Assessment criteria for [NKEV-INIT-UPD]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [NKEV-INIT-UPD];
- a functional sufficiency assessment the personal wearable's behaviour on first start or after factory reset to fulfil [NKEV-INIT-UPD];

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

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

The following test setups shall be prepared:

- personal wearable in its default configuration
- documented interfaces and network connections used by software update mechanisms or notification mechanisms

**Assessment activities:**

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

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

## 6.4 Secure by default configuration

### 6.4.1 Assessment criteria for [SDC-AUM-FH]

**Assessment objective:**

The assessment covers:

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

based on the factory default state.

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

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

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

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

The following test setups shall be prepared:

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

**Assessment activities:**

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

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

### 6.4.2 Assessment criteria for [SDC-SUM-AUTO]

**Assessment objective:**

The assessment covers:

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

based on the factory default state.

**Assessment preparation:**

The following documentation for the personal wearable's shall be complete for each architectural component:

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

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

The following test setups shall be prepared:

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

**Assessment activities:**

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

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

### 6.4.3 Assessment criteria for [SDC-SUM-NOTIF]

**Assessment objective:**

The assessment covers:

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

based on the factory default state.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- documentation describing all supported software update notification mechanisms where software update notification is used in the factory default state or whose use can be activated during initialisation, including:
  - a description of how software update notifications are triggered; and
  - a description of how notifications are received; and
- documentation describing parts of the personal wearable's updatable software where software update notification is not used in the factory default state or whose use can not be activated during initialisation, including:
  - (if the personal wearable does not use software update notification in the factory default state or whose use can not be activated during initialisation for an updatable part of its software);
  - a justified statement that each of the personal wearable's architectural component has no capability to connect to public networks.

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

The following test setups shall be prepared:

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

**Assessment activities:**

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

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

### 6.4.4 Assessment criteria for [SDC-FRM]

**Assessment objective:**

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

**Assessment preparation:**

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

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

**Assessment activities:**

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

**Assessment verdict:**

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- Description of the performed test
- All test records of the performed test

### 6.4.5 Assessment criteria for [SDC-PARCONT]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [SDC-PARCONT];
- a functional completeness assessment on the personal wearable capabilities that are addressed by [SDC-PARCONT];

based on the default configuration required by clause 5.4.

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

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

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

The following test setups shall be prepared:

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

**Assessment activities:**

- The personal wearable's conformity to [SDC-PARCONT] shall be validated based on the documentation.

- The correctness and completeness of the documentation shall be verified by:
  - inspecting the personal wearable in factory default state; and
  - (if parental control functions can be configured during initialisation) performing the initialisation without providing explicit confirmation of configurations after initialisation; and
  - an inspection of the personal wearable for functions, corresponding parental control functions and associated parental control configuration possibilities that are accessible via human interfaces.

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

### 6.4.6 Assessment criteria for [SDC-MON-HANDLE]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of each audit event data generated by a monitoring mechanism of the personal wearable to fulfil [SDC-MON-HANDLE];

based on the default configuration required by clause 5.4.

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

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

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

The following test setups shall be prepared:

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

**Assessment activities:**

The following activities shall be performed:

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

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

Descriptions of the performed tests and records of performed tests.

### 6.4.7 Assessment criteria for [CRY-SOTA]

Compliance with [CRY-GENERAL] shall be assessed according to the assessment criteria provided in Annex K.

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

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [CRY-CCK-PRE-LEN];
- a functional completeness assessment on the personal wearable's preinstalled long term confidential cryptographic keys;

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- a list of personal wearable's preinstalled long term confidential cryptographic keys;
- for each preinstalled long term confidential cryptographic key:
  - a description of generation method of the confidential cryptographic key;
  - its key sizes and corresponding security strength including a justification for the security strength;
- for each architectural component, a test setup for identifying and analyzing preinstalled long term confidential cryptographic keys;

**Assessment activities:**

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

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

### 6.4.9 Assessment criteria for [CRY-CCK-GEN]

**Assessment objective:**

The assessment covers:

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

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

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

The following test setups shall be prepared:

- for each personal wearable's long term confidential cryptographic key generation mechanism, a test setup for generating and extracting corresponding long term confidential cryptographic keys based on a sample personal wearable in default configuration;

**Assessment activities:**

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

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

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

**Assessment objective:**

The assessment covers:

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

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- a list of personal wearable's preinstalled passwords;
- for each preinstalled password:
  - a description of generation method of the password;
  - its complexity and the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) for the corresponding authentication mechanisms' usage, including a justification for the password's complexity.
- for each architectural component, a test setup for identifying and analyzing preinstalled passwords;

**Assessment activities:**

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

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- records of the validation of the documentation;

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

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

**Assessment objective:**

The assessment covers:

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

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

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

The following test setups shall be prepared:

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

**Assessment activities:**

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

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

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

**Assessment objective:**

The assessment covers:

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

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

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

The following test setups shall be prepared:

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

**Assessment activities:**

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

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

## 6.5 Security updates

### 6.5.1 Assessment criteria for [SU-SUPPORT]

**Assessment objective:**

The assessment covers:

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

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

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

The following test setups shall be prepared:

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

**Assessment activities:**

The following activities shall be performed:

- The personal wearable's conformity to [SU-SUPPORT] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by:
  - inspecting the personal wearable to identify software architectural components.

- For each software update mechanism, its correct implementation shall be verified by:
  - installing an update over this software update mechanism to update a software architectural component; and
  - checking whether the software has changed to the updated software.

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

### 6.5.2 Assessment criteria for [SU-PROVIDE]

**Assessment objective:**

The assessment covers:

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

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

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

The following test setups shall be prepared:

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

**Assessment activities:**

The following activities shall be performed:

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

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

### 6.5.3 Assessment criteria for [SU-AUTO]

**Assessment objective:**

The assessment covers:

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

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

**Assessment preparation:**

The following documentation for the personal wearable shall be complete for each architectural component:

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

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

The following test setups shall be prepared:

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

**Assessment activities:**

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

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

### 6.5.4 Assessment criteria for [SU-DISABLE-AUTO]

**Assessment objective:**

The assessment covers:

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

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

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

The following test setups shall be prepared:

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

**Assessment activities:**

The following activities shall be performed:

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

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

### 6.5.5 Assessment criteria for [SU-POSTPONE-AUTO]

**Assessment objective:**

The assessment covers:

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

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- list of all software update mechanism that support automated security updates;

- documentation on how to postpone automated updates;
- documentation on entities intended to operate the personal wearable.

The following test setups shall be prepared:

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

**Assessment activities:**

The following activities shall be performed:

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

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

### 6.5.6 Assessment criteria for [SU-NOTIF]

**Assessment objective:**

The assessment covers:

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

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- documentation describing all supported software update notification mechanisms, including:
  - a description of how software update notifications are triggered; and

  - a description of how notifications are received; and

- documentation describing parts of the personal wearable's updatable software where software update notification is not supported:

  - (if the personal wearable does not support software update notification for an updatable part of its software);

  - a justified statement that each of the personal wearable's architectural component has no capability to connect to public networks.

The following test setups shall be prepared:

- for each software update notification mechanism:

  - a test setup that allows to trigger update notifications; and

  - a test setup that allows to receive update notifications based on a sample personal wearable in default configuration.

**Assessment activities:**

- The personal wearable's conformity to [SU-NOTIF] shall be validated based on the documentation.

- For each software update notification mechanism, its correct implementation shall be verified by:

  - triggering a software update notification; and

  - checking whether the software update notification mechanism automatically notifies the personal wearable's users that an update of its software is available.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the documentation indicates the personal wearable's conformity with [SU-NOTIF]; and

- the verification of the correct implementation of each software update notification mechanism was successful.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- records of the validation of the documentation;

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

## 6.6 Authentication and access control

### 6.6.1 Assessment criteria for [ACM-FH]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [ACM-FH];

- a functional completeness assessment on the personal wearable capabilities that are addressed by [ACM-FH];

- a functional sufficiency assessment of each access control mechanism used by the personal wearable to fulfil [ACM-FH];

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

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

The following test setups shall be prepared:

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

**Assessment activities:**

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

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the documentation indicates the personal wearable's conformity to [ACM-FH]; and
- the verification of the correctness and completeness of the documentation was successful; and
- the verification of the correct implementation of each access control mechanism was successful.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

### 6.6.2 Assessment criteria for [AUM-FH]

**Assessment objective:**

The assessment covers:

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

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- a list of personal wearable's functions whose use can cause harm;
- for each function, whose use can cause harm:
  - its impact class IMP.FH;
  - the physical operational environment of the architectural component that performs the function;
  - for each of the function's trigger input possibilities:
    - the interface and communication type;
    - a list of corresponding authentication mechanisms including:
      - the authentication mechanisms' strength;
      - the type of authentication factors;
      - the documentation defined in the corresponding assessments in clause E.1.2 in *Assessment preparation.*

The following test setups shall be prepared:

- a test setup for identifying functions, their trigger input possibilities and corresponding authentication mechanisms based on a sample personal wearable in default configuration;
- for each authentication mechanism, a test setup defined by the test cases provided in clause E.1 according to the needs determined by its strength and the type of its authentication factors.

**Assessment activities:**

- The personal wearable's conformity to [AUM-FH] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by:
  - an inspection of the personal wearable for functions and related authentication mechanisms that are accessible via physical human interfaces;
  - a scan of the personal wearable for functions and related authentication mechanisms that are accessible via logical interfaces.
- For each authentication mechanism, its correct implementation shall be verified based on the test cases provided in clause E.1 according to the needs determined by its strength and the type of its authentication factors.

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

### 6.6.3 Assessment criteria for [AUTHZ-LP]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [AUTHZ-LP];

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

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

**Assessment activities:**

- The personal wearable's conformity to [AUTHZ-LP] shall be validated based on the documentation.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the documentation indicates the personal wearable's conformity to [AUTHZ-LP].

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- records of the validation of the documentation.

### 6.6.4 Assessment criteria for [AUTHZ-R]

**Assessment objective:**

The assessment covers:

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

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

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

The following test setups shall be prepared:

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

**Assessment activities:**

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

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

### 6.6.5 Assessment criteria for [PARCONT]

**Assessment objective:**

The assessment covers:

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

based on the default configuration required by clause 5.4.5.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

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

The following test setups shall be prepared:

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

**Assessment activities:**

- The personal wearable's conformity to [PARCONT] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by:
  - an inspection of the personal wearable for functions, corresponding parental control functions and associated parental control configuration possibilities that are accessible via human interfaces.
- For each function that is intended to be used by children, its correct implementation of corresponding parental control functions and associated parental control configuration possibilities shall be verified by:
  - performing changes to the parental control configuration via the corresponding parental control functions'; and
  - assessing the enforcement of the parental control configuration changes from a child's perspective.

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

descriptions of the performed tests and documentation of associated test records that verify the correct implementation of the parental control functions.

### 6.6.6 Assessment criteria for [AUTHZ-PC]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of the personal wearable's authorisation policy to fulfil [AUTHZ-PC].

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- a list of the personal wearable's parental control functions.

The following test setups shall be prepared:

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

**Assessment activities:**

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

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

## 6.7 Confidentiality protection

### 6.7.1 Assessment criteria for [CONF-SSM]

**Assessment objective:**

The assessment covers:

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

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

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

The following test setups shall be prepared:

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

**Assessment activities:**

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

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the documentation indicates the personal wearable's conformity to [CONF-SSM]; and
- the verification of the correctness and completeness of the documentation was successful; and
- the verification of the correct implementation of each confidentiality protecting secure storage mechanism was successful.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

### 6.7.2 Assessment criteria for [CONF-COM]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [CONF-COM];
- a functional completeness assessment on the personal wearable capabilities that are addressed by [CONF-COM];
- a functional sufficiency assessment of each confidentiality protecting communication mechanism used by the personal wearable to fulfil [CONF-COM];

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- a list of personal wearable's confidential data that are intended to be communicated by or to the personal wearable;
- for each confidential data that are intended to be communicated by or to the personal wearable:
  - its impact class IMP.CONF;
  - a list of architectural components that can communicate the confidential data including:
    - its physical operational environment;
    - the corresponding interfaces and communication types;
    - a list of corresponding confidentiality protecting communication mechanisms including their strengths.

The following test setups shall be prepared:

- for each architectural component, a test setup based on a sample personal wearable in default configuration for identifying:
  - confidential data that can be communicated by or to the architectural component;
  - the corresponding interfaces and communication types for communication;
  - the corresponding confidentiality protecting communication mechanisms;
- for each confidentiality protecting communication mechanism, a test setup defined by the test cases provided in clause E.3 according to the needs determined by its strength.

**Assessment activities:**

- The personal wearable's conformity to [CONF-COM] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by:
  - an inspection of the personal wearable's physical human interfaces for communicable confidential data, related communication capabilities and confidentiality protecting communication mechanisms;
  - a scan of the personal wearable's logical interfaces for communicable confidential data, related communication capabilities and confidentiality protecting communication mechanisms.
- For each confidentiality protecting communication mechanism, its correct implementation shall be verified based on the test cases provided in clause E.3 according to the needs determined by its strength.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the documentation indicates the personal wearable's conformity to [CONF-COM]; and
- the verification of the correctness and completeness of the documentation was successful; and
- the verification of the correct implementation of each confidentiality protecting communication mechanism was successful.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- records of the validation of the documentation;

- descriptions of the performed tests and records of performed tests to verify the correctness and completeness of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each confidentiality protecting communication mechanism.

### 6.7.3 Assessment criteria for [CONF-MON-HW]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [CONF-MON-HW]; and
- a functional sufficiency assessment to fulfil [CONF-MON-HW];

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- documentation of event detection based on continuously captured private audio data or private video data on a hardware architectural component;
- documentation on visual or auditory indicators with corresponding hardware architectural component;
- documentation which visual or auditory indicator is used for which event detection.

The following test setups shall be prepared:

- for each documented event detection loop a test setup with the permissions to:
  - trigger processing beyond the event detection loop and access to the documented corresponding used visual or auditory indicators; and
  - access the information which processing beyond the event detection loop is active.

**Assessment activities:**

The following activities shall be performed:

- The personal wearable's conformity to [CONF-MON-HW] shall be validated based on the documentation.
- For each documented event detection loop on a hardware architectural component
  - verify that the processing beyond the event detection loop is not active and the documented indicator is not active;
  - trigger the processing beyond the event detection loop; and
  - verify that the processing beyond the event detection loop is active and the documented indicator is active.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the documentation indicates the personal wearable's conformity to [CONF-MON-HW]; and
- the verification of the correct implementation of each visual or auditory indication on processing beyond the event detection loop was successful.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- records of the validation of the documentation;

descriptions of the performed tests and records of performed tests.

# 6.8 Integrity protection

## 6.8.1 Assessment criteria for [INT-SSM]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [INT-SSM];
- a functional completeness assessment on the personal wearable capabilities that are addressed by [INT-SSM];
- a functional sufficiency assessment of each integrity protecting secure storage mechanism used by the personal wearable to fulfil [INT-SSM];

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- a list of personal wearable's integrity relevant data that are intended to be persistently stored by the personal wearable;
- for each integrity relevant data that are intended to be persistently stored by the personal wearable:
  - its impact class IMP.INT;
  - a list of architectural components that store the integrity relevant data including:
    - its physical operational environment;
    - a list of storage locations for the integrity relevant data;
    - a list of corresponding integrity protecting secure storage mechanisms including their strengths.

The following test setups shall be prepared:

- for each architectural component, a test setup for identifying integrity relevant data, their storage location and corresponding integrity protecting secure storage mechanisms based on a sample personal wearable in default configuration;
- for each integrity protecting secure storage mechanism, a test setup defined by the test cases provided in clause E.2 according to the needs determined by its strength.

**Assessment activities:**

- The personal wearable's conformity to [INT-SSM] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by:
  - an inspection of the personal wearable's physical human interfaces for persistently storable/stored integrity relevant data, related storage locations and integrity protecting secure storage mechanisms;
  - a scan of the personal wearable's logical interfaces for persistently storable/stored integrity relevant data, related storage locations and integrity protecting secure storage mechanisms.
- For each integrity protecting secure storage mechanism, its correct implementation shall be verified based on the test cases provided in clause E.2 according to the needs determined by its strength.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the documentation indicates the personal wearable's conformity to [INT-SSM]; and
- the verification of the correctness and completeness of the documentation was successful; and
- the verification of the correct implementation of each integrity protecting secure storage mechanism was successful.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

### 6.8.2 Assessment criteria for [INT-SWPCK]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [INT-SWPCK];
- a functional completeness assessment on the personal wearable capabilities that are addressed by [INT-SWPCK];
- a functional sufficiency assessment of each software package verification mechanism used by the personal wearable to fulfil [INT-SWPCK];

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- a list of the personal wearable's architectural components;
- for each architectural component:
  - a list of mechanisms to install software packages;
  - for each personal wearable's mechanism to install software packages:
    - the communication types of over which software packages can be received;
    - a list of software that can be installed by the mechanism including the maximum impact class IMP.INT of corresponding software packages;
    - a list of corresponding software package verification mechanisms including their strengths.

The following test setups shall be prepared:

- for each architectural component, a test setup for identifying mechanisms to install software packages, corresponding software that can be installed, communication types of over which corresponding software packages can be received and corresponding software package verification mechanisms based on a sample personal wearable in default configuration;

- for each mechanism to install software packages, a test setup defined by the test cases provided in clause E.2 according to the needs determined by its strength.

**Assessment activities:**

- The personal wearable's conformity to [INT-SWPCK] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by:
  - an inspection of the personal wearable's physical human interfaces for mechanism to install software packages;
  - a scan of the personal wearable's logical interfaces for mechanism to install software packages;
  - for each mechanism to install software packages, performing the installation of a software package to identify software package verification mechanisms.
- For each software package verification mechanism, its correct implementation shall be verified based on the test cases provided in clause E.2 according to the needs determined by its strength.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the documentation indicates the personal wearable's conformity to [INT-SWPCK]; and
- the verification of the correctness and completeness of the documentation was successful; and
- the verification of the correct implementation of each software package verification mechanism was successful.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

descriptions of the performed tests and records of performed tests to verify the correct implementation of each software package verification mechanism.

### 6.8.3 Assessment criteria for [INT-COM]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [INT-COM];
- a functional completeness assessment on the personal wearable capabilities that are addressed by [INT-COM];
- a functional sufficiency assessment of each integrity protecting communication mechanism used by the personal wearable to fulfil [INT-COM];

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- a list of personal wearable's integrity relevant data that are intended to be communicated by or to the personal wearable;

- for each integrity relevant data that are intended to be communicated by or to the personal wearable:
  - its impact class IMP.CONF;
  - a list of architectural components that can communicate the integrity relevant data including:
    - its physical operational environment;
    - the corresponding interfaces and communication types;
    - a list of corresponding integrity protecting communication mechanisms including their strengths.

The following test setups shall be prepared:

- for each architectural component, a test setup based on a sample personal wearable in default configuration for identifying:
  - integrity relevant data that can be communicated by or to the architectural component;
  - the corresponding interfaces and communication types for communication;
  - the corresponding integrity protecting communication mechanisms;
- for each integrity protecting communication mechanism, a test setup defined by the test cases provided in clause E.2 according to the needs determined by its strength.

**Assessment activities:**

- The personal wearable's conformity to [INT-COM] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by:
  - an inspection of the personal wearable's physical human interfaces for communicable integrity relevant data, related communication capabilities and integrity protecting communication mechanisms;
  - a scan of the personal wearable's logical interfaces for communicable integrity relevant data, related communication capabilities and integrity protecting communication mechanisms.
- For each integrity protecting communication mechanism, its correct implementation shall be verified based on the test cases provided in clause E.2 according to the needs determined by its strength.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the documentation indicates the personal wearable's conformity to [INT-COM]; and
- the verification of the correctness and completeness of the documentation was successful; and
- the verification of the correct implementation of each integrity protecting communication mechanism was successful.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

## 6.9 Data minimisation

### 6.9.1 Assessment criteria for [DMIN-DJST]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of Minimise processed data

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- a list of all data assets processed by the personal wearable whose impact class for confidential personal wearable data is IMP.CONF.Low or higher;
- for each documented confidential data asset, the associated rationale for its necessity explaining why its processing is necessary for the intended purpose of the personal wearable.

**Assessment activities:**

- the personal wearable's conformity to [DMIN-DJST] shall be validated based on the documentation

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the documentation indicates the personal wearable's conformity to [DMIN-DJST];

Otherwise, the verdict FAIL shall be assigned.

**Assessment evidence:**

- records of the validation of the documentation

## 6.10 Availability protection

### 6.10.1 Assessment criteria for [AVAI-TIME-RECO-POW]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of the recovery function interaction with each power supply used by the personal wearable's hardware architectural components to fulfil [AVAI-TIME-RECO-POW];

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- a list of all personal wearable's hardware architectural components;
- for each personal wearable's hardware architectural component:
  - a list of all power supplies
  - for each power supply:
    - a description whether the power supply can power the hardware architectural component alone

- a list of all functionalities of the personal wearable that need communication involving the hardware architectural component:
    - for each of these functionalities:
        - a list of interfaces of the personal wearable, where the connection status of the necessary communication channels can be read; or
        - parameters of the necessary communication channels of the hardware architectural components in order to externally observe if the connection is active;
        - a list of interfaces of the personal wearable, where the operational status of the hardware architectural components can be read:
            - description how the operational status can be implied from the interface readings.

The following test setups shall be prepared:

- the personal wearable is set up in default configuration;
- a test setup to:
    - safely disconnect or disable and reconnect or enable the power supplies of the personal wearable's hardware architectural components;
    - enable access to at least one interfaces of the personal wearable, where the operational status of the personal wearable can be read;
    - enable access to at least one interfaces of the personal wearable, where the connection status the necessary communication channels status of the hardware architectural components can be read;
    - if the connection status for all necessary communication channels of the hardware architectural components cannot be read from the personal wearable:
        - monitor whether all necessary communication channels of the hardware architectural components are active.

**Assessment activities:**

The following activities shall be performed for each hardware architectural component:

- for every possible order in which the hardware architectural component power supplies can be disconnected or disabled:
    - disconnect or disable all power supplies of the hardware architectural component
    - wait at least 30 s
    - reconnect or enable the power supplies
    - monitor the operational status of the personal wearable
    - monitor the connection status for all necessary communication channels of the hardware architectural component
    - record the order in which the power supplies are disconnect or disable and reconnect or enable
    - record the time relative to the reconnection or enabling of the last power supply, after which the personal wearable indicates, that it is operational and all necessary communication channels are established; OR
    - record the time relative to the reconnection or enabling of the last power supply, after which every necessary communication channel of the hardware architectural component was active at least once, and there is no indication that the personal wearable has not resumed operation

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the personal wearable signals resume of operations and establishment of all necessary communication channels within one hour after the reconnection or enabling of the last power supply; or
- all necessary communication channels of the hardware architectural components were active at least once, and there is no indication that the personal wearable has not resumed operation within one hour;
- the verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- descriptions of the performed tests and records of performed tests

## 6.10.2 Assessment criteria for [AVAI-TIME-NETW]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [AVAI-TIME-NETW];
- a functional completeness assessment on the personal wearable capabilities that are addressed by [AVAI-TIME-NETW];
- a functional sufficiency assessment of each time sensitive function without the need of network connectivity to operate used by the personal wearable to fulfil [AVAI-TIME-NETW];

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- a list of all time sensitive function of the personal wearable:
- for each time sensitive function:
  - description of the functionalities realised or supported by this function
  - list of interfaces necessary for the operation of this function:
    - for each interface:
    - communication types of the interface
- a list of interfaces of the personal wearable, where the status of the architectural component's time sensitive function can be read:
  - description how the status can be implied from the interface readings

The following test setups shall be prepared:

- the personal wearable is set up in default configuration
- a test setup to:
  - disconnect or disable the public communication of the personal wearable's architectural components
  - disconnect or disable the adjacent communication of the personal wearable's architectural components
  - enable access to at least one interfaces of the personal wearable, where the status of the personal wearable's time sensitive function can be read

**Assessment activities:**

The following activities shall be performed:

- verify the correctness and completeness of the documentation
- repeat the following steps for communication types public communication, adjacent communication and both, depending on the communication type needed by the functions to be tested:
  - disconnect or disable the corresponding communication type of the personal wearables architectural component
  - wait at least 30 s
  - for each time sensitive function which does not need any interface with the corresponding communication type for its operation:
    - check whether the function is in operable status
    - record the status of the function and the disconnected or disabled communication type
  - reconnect or enable the corresponding communication type

**Assessment verdict:**

The verdict PASS shall be assigned if:

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

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- descriptions of the performed tests and records of performed tests

### 6.10.3 Assessment criteria for [AVAI-TIME-RECO-NETW]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [AVAI-TIME-RECO-NETW]
- a functional completeness assessment on the personal wearable capabilities that are addressed by [AVAI-TIME-RECO-NETW]
- a functional sufficiency assessment of the personal wearables architectural components recovery after loss of network connection, to fulfil [AVAI-TIME-RECO-NETW]

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- a list of all functions of the personal wearable that need communication involving the architectural component:
  - for each of these functions:
    - list of interfaces involving the architectural component and are necessary for the operation of this function:
      - for each interface:
      - communication types of the interface

- a list of interfaces of the personal wearable, where the connection status of the necessary communication channels can be read; or
- parameters of the necessary communication channel of the architectural component in order to externally observe if the connection is active

The following test setups shall be prepared:

- the personal wearable is set up in default configuration
- a test setup to:
  - disconnect or disable the public communication of the personal wearables architectural component
  - disconnect or disable the adjacent communication of the personal wearables architectural component
  - enable access to at least one interfaces of the personal wearable, where the connection status the necessary interfaces involving the architectural component and are necessary for the operation of these functions can be read; or
  - if the connection status for all necessary interfaces involving the architectural component and are necessary for the operation of these functions cannot be read from the personal wearable:
    - monitor whether all necessary interfaces involving the architectural component and are necessary for the operation of these functions

**Assessment activities:**

The following activities shall be performed:

- verify the correctness and completeness of the documentation by:
  - check for undocumented interfaces
- repeat the following steps for communication types public communication, adjacent communication and both at the same time:
  - disconnect or disable the corresponding communication type of the personal wearables architectural component
  - wait at least 60 s
  - reconnect or enable the corresponding communication type
  - record the corresponding communication type
  - for each documented function:
    - monitor the operational status of the function
    - for each interface necessary for the operation of this function:
      - monitor the connection status
      - record the time relative to the reconnection or enabling of the corresponding communication type, after which the personal wearable indicates, that the interface is reconnected; or
      - record the time relative to the reconnection or enabling of the corresponding communication type, after which the interface was active at least once, and there is no indication that the personal wearable has not resumed operation

**Assessment verdict:**

The verdict PASS shall be assigned if:

- no indication, that the documentation is incorrect or incomplete, are found; and

- the personal wearable signals resume of operations and establishment of all necessary communication channels within one hour; or
- all necessary communication channels of the architectural component were active at least once, and there is no indication that the personal wearable has not resumed operation within one hour
- the verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- descriptions of the performed tests and records of performed tests

### 6.10.4 Assessment criteria for [AVAI-TIME-OUTA-NOT]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [AVAI-TIME-OUTA-NOT]
- a functional sufficiency assessment of the personal wearables notification in case of non-availability induced by network resource restrictions, to fulfil [AVAI-TIME-OUTA-NOT]
- a functional sufficiency assessment of the personal wearables notification in case of non-availability induced by DOS, to fulfil [AVAI-TIME-PREV-NOT]

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- description how the status of the personal wearables time sensitive functions can be read or deduced
- a list of all time sensitive functions of the personal wearable:
  - for each of these functions:
    - the time sensitive availability impact class
    - whether the function needs network connectivity
- CPU, memory, power and network resources available to the personal wearable
- demands on CPU, memory, power and network resources for workload consistent with the personal wearables intended purpose and reasonably foreseeable use
- a list of all notification mechanisms of the personal wearable:
  - description how the notification mechanism can be configured

The following test setups shall be prepared:

- the personal wearable is set up in default configuration
- configure at least one notification mechanism
- a test setup to:
  - limit the network bandwidth between the personal wearables architectural component and the personal wearables RDPS to the internet
  - induce a denial-of-service status on the personal wearable causing increasing demand on processing resources
  - receive notifications from the personal wearable

**Assessment activities:**

The following activities shall be performed:

- verify the correctness and completeness of the documentation
- conceptually verify whether the documented notification mechanisms are suitable to send notifications in case of resource limitations
- if at least on time sensitive function needs network connectivity:
  - progressively lower the network bandwidth available to the personal wearables architectural component:
    - record any received notifications form the personal wearable
  - progressively higher the intensity of requests to induce a denial-of-service status on the personal wearable:
    - record any received notifications form the personal wearable

**Assessment verdict:**

The verdict PASS shall be assigned if:

- no indication, that the documentation is incorrect or incomplete, are found; and
- the personal wearable sends notifications according to its configuration in case of non-availability of time sensitive function with IMP.AVAI.TIME.Medium or higher induced by DOS; or
  - no time sensitive function with IMP.AVAI.TIME.Medium or higher was non-availability due to DOS; and
- the personal wearable sends notifications according to its configuration in case of non-availability of time sensitive function with IMP.AVAI.TIME.Medium or higher induced by network bandwidth limitation; or
  - no time sensitive function with IMP.AVAI.TIME.Medium or higher was non-availability due to network bandwidth limitation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- descriptions of the performed tests and records of performed tests

### 6.10.5 Assessment criteria for [AVAI-TIME-PREV-NOT]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [AVAI-TIME-PREV-NOT]
- a functional sufficiency assessment of the personal wearables notification in case of network resource restrictions, to fulfil [AVAI-TIME-PREV-NOT]
- a functional sufficiency assessment of the personal wearables notification in case of DOS, to fulfil [AVAI-TIME-PREV-NOT]

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- a list of all time sensitive functions of the personal wearable:
  - for each of these functions:
    - the time sensitive availability impact class
    - whether the function needs network connectivity
- CPU, memory, power and network resources available to the personal wearable
- demands on CPU, memory, power and network resources for workload consistent with the personal wearables intended purpose and reasonably foreseeable use
- a list of all notification mechanisms of the personal wearable:
  - description how the notification mechanism can be configured

The following test setups shall be prepared:

- the personal wearable is set up in default configuration
- configure at least one notification mechanism
- a test setup to:
  - read or deduced the status of the time sensitive functions from the personal wearable
  - limit the network bandwidth between the personal wearables architectural component and the personal wearables RDPS to the internet
  - induce a DOS status on the personal wearable causing increasing demand on processing resources
  - receive notifications from the personal wearable

**Assessment activities:**

The following activities shall be performed:

- verify the correctness and completeness of the documentation
- conceptually verify whether the documented notification mechanisms are suitable to send notifications in case of resource limitations
- if at least on time sensitive function needs network connectivity:
  - progressively lower the network bandwidth available to the personal wearables architectural component:
    - record any received notifications form the personal wearable
  - progressively higher the intensity of requests to induce a DOS status on the personal wearable:
    - record any received notifications form the personal wearable

**Assessment verdict:**

The verdict PASS shall be assigned if:

- no indication, that the documentation is incorrect or incomplete, are found; and
- the personal wearable sends notifications according to its configuration in case of resource limitations induced by DOS; and

- the personal wearable sends notifications according to its configuration in case of network bandwidth limitation; or
    - no time sensitive function with IMP.AVAI.TIME.High of the personal wearable of the personal wearable needs network connectivity.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- descriptions of the performed tests and records of performed tests

## 6.10.6 Assessment criteria for [AVAI-TIME-RES-PRIO]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [AVAI-TIME-RES-PRIO]
- a functional sufficiency assessment of the personal wearables resource prioritisation in case of non-availability induced by DOS, to fulfil [AVAI-TIME-RES-PRIO]

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- description how the status of the personal wearables time sensitive functions can be read or deduced
- a list of all time sensitive functions of the personal wearable:
    - for each of these functions:
        - the time sensitive availability impact class
        - whether the function needs network connectivity
- prioritisation policy for the time sensitive functions of the personal wearable in case of CPU, memory or power resource conflict

The following test setups shall be prepared:

- the personal wearable is set up in default configuration
- a test setup to:
    - read or deduced the status of the time sensitive functions from the personal wearable
    - induce a DOS status on the personal wearable causing increasing demand on processing resources

**Assessment activities:**

The following activities shall be performed:

- verify the correctness and completeness of the documentation
- conceptually verify the prioritisation policy
- progressively higher the intensity of requests to induce a DOS status on the personal wearable:
    - record the status of every time sensitive function

**Assessment verdict:**

The verdict PASS shall be assigned if:

- no indication, that the documentation is incorrect or incomplete, are found; and
- the prioritisation policy is conceptually valid; and
- every time sensitive function:
  - the status of the function is in accordance with the prioritisation policy during DOS.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- descriptions of the performed tests and records of performed tests

### 6.10.7 Assessment criteria for [AVAI-TIME-RES-PRIO]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [AVAI-TIME-RES-PRIO]
- a functional sufficiency assessment of the wearables resource prioritization in case of non-availability induced by DOS, to fulfil [AVAI-TIME-RES-PRIO]

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the wearable shall be complete:

- description how the status of the wearables time sensitive functions can be read or deduced
- a list of all time sensitive functions of the wearable:
  - for each of these functions:
    - the time sensitive availability impact class
    - whether the function needs network connectivity
- prioritization policy for the time sensitive functions of the wearable in case of CPU, memory or power resource conflict

The following test setups shall be prepared:

- the wearable is set up in default configuration
- a test setup to:
  - read or deduced the status of the time sensitive functions from the wearable
  - induce a DOS status on the wearable causing increasing demand on processing resources

**Assessment activities:**

The following activities shall be performed:

- verify the correctness and completeness of the documentation
- conceptually verify the prioritization policy

- progressively higher the intensity of requests to induce a DOS status on the wearable:
  - record the status of every time sensitive function

**Assessment verdict:**

The verdict PASS shall be assigned if:

- no indication, that the documentation is incorrect or incomplete, are found; and
- the prioritization policy is conceptually valid; and
- every time sensitive function:
  - the status of the function is in accordance with the prioritization policy during DOS.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- Descriptions of the performed tests and records of performed tests

### 6.10.8 Assessment criteria for [AVAI-SUM-SCHEDULE]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [AVAI-SUM-SCHEDULE]
- a functional sufficiency assessment of the personal wearables notification in case of non-availability induced by DOS, to fulfil [AVAI-TIME-PREV-NOT]

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- a list of all time sensitive functions of the personal wearable:
  - for each of these functions:
    - the time sensitive availability impact class
- a list of all software update mechanisms of the personal wearable:
  - for each of these mechanisms:
    - whether this mechanism can effect at least one time sensitive function with IMP.AVAI.TIME.Medium or higher
    - description how the software update mechanism can be configured

The following test setups shall be prepared:

- the personal wearable is set up in default configuration

**Assessment activities:**

The following activities shall be performed:

- verify the correctness and completeness of the documentation

- for every software update mechanism that can effect at least one time sensitive function with IMP.AVAI.TIME.Medium or higher:
  - check whether the application of software updates can be scheduled
  - record the results

**Assessment verdict:**

The verdict PASS shall be assigned if:

- no indication, that the documentation is incorrect or incomplete, are found; and
- for every software update mechanism that can effect at least one time sensitive function with IMP.AVAI.TIME.Medium or higher:
  - the application of software updates can be scheduled

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- descriptions of the performed tests and records of performed tests

## 6.11 Non-interference

Not applicable see Annex A.

## 6.12 Attack surface minimisation

### 6.12.1 Assessment criteria for [LAS-INVAL]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [LAS-INVAL]
- a functional sufficiency assessment of the input validation mechanisms used by the personal wearable to fulfil [LAS-INVAL]

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for each personal wearable's function that uses external data input:
  - a list of all interfaces over which these functions can receive external data input, including their communication type
  - a description of the personal wearable's input validation mechanisms

The following test setups shall be prepared:

- For each personal wearable's functions that use external data input:
  - For each interfaces over which these functions can receive external data input:
    - a test setup to send external data input that does not meet an input validation mechanism's acceptance pattern based on a sample personal wearable in default configuration.

**Assessment activities:**

- For each personal wearable's function that uses external data input, the personal wearable's conformity to [LAS-INVAL] shall be validated based on the documentation by:
  - For each interface over which these functions can receive external data input:
    - verify whether the interface has COM.StrictLocal
    - For each interface that does not have COM.StrictLocal:
      - verify the existence of input validation mechanisms
- For each input validation mechanism, its correct implementation shall be verified by:
  - sending data input that does not meet an input validation mechanism's acceptance pattern and assessing the personal wearable's behaviour.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the documentation indicates the personal wearable's conformity to [LAS-INVAL]; and
- the verification of the correct implementation of each input validation mechanism was successful.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- records of the validation of the documentation
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each input validation mechanism

### 6.12.2 Assessment criteria for [LAS-INSAN]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [LAS-INSAN]
- a functional sufficiency assessment of the input sanitisation mechanisms used by the personal wearable to fulfil [LAS-INSAN]

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for each personal wearable's function that uses external data input:
  - a description of the personal wearable's input sanitisation mechanisms; or
  - an explanation of the input validation mechanisms capability to prevent potential incidents triggered by external data input.

The following test setups shall be prepared:

- For each personal wearable's functions that use external data input:
  - For each interfaces over which these functions can receive external data input:
    - a test setup to send external data input that includes common code injection patterns based on a sample personal wearable in default configuration.

**Assessment activities:**

- For each personal wearable's function that uses external data input, the personal wearable's conformity to [LAS-INSAN] shall be validated based on the documentation by:
  - For each interface over which these functions can receive external data input:
    - verify the existence of input sanitisation mechanisms; or
    - verify that the explanation of the input validation mechanisms capability to prevent potential incidents triggered by external data input.
- For each input sanitisation mechanism, its correct implementation shall be verified by:
  - sending data input that include common code injection patterns and assessing the personal wearable's behaviour.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the documentation indicates the personal wearable's conformity to [LAS-INSAN]; and
- the verification of the correct implementation of each input sanitisation mechanism was successful.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- records of the validation of the documentation
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each input sanitisation mechanism

### 6.12.3 Assessment criteria for [LAS-PHY-INF]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [LAS-PHY-INF]; and
- a functional completeness assessment on the personal wearable's capabilities that are addressed by [LAS-PHY-INF].

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- a list of all physical interfaces that are provided by hardware architectural components, and
- for each physical interface:
  - a justification for its necessity for the personal wearable's intended purpose

The following test setup shall be prepared:

- hardware architectural components, and
- appropriate inspection equipment and tools to identify physical interfaces, including those potentially concealed behind covers, seals, etc.

**Assessment activities:**

- The personal wearable's conformity to [LAS-PHY-INF] shall be validated based on the documentation.

- The correctness and completeness of the documentation shall be verified by inspecting the hardware architectural components.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the documentation indicates the personal wearable's conformity to [LAS-PHY-INF]; and
- the verification of the correctness and completeness of the documentation was successful.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- photographs/annotated drawings of all discovered physical interfaces
- records of the validation of the documentation
- descriptions of the performed inspection

### 6.12.4 Assessment criteria for [LAS-LOGIC-INF]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [LAS-LOGIC-INF]; and
- a functional completeness assessment on the personal wearable's capabilities that are addressed by [LAS-LOGIC-INF].

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- a list of all logical interfaces that are provided by default, and
- for each logical interface provided by default:
  - a justification for its necessity for the personal wearable's intended purpose

The following test setup shall be prepared:

- a test setup for identifying logical interfaces based on a sample personal wearable in default configuration

NOTE: Such a test setup can amongst others include network scanning tools, protocol-specific discovery tools (e.g. for UPnP discovery) and API probing tools.

**Assessment activities:**

- The personal wearable's conformity to [LAS-LOGIC-INF] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by inspecting the personal wearable.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the documentation indicates the personal wearable's conformity to [LAS-LOGIC-INF]; and
- the verification of the correctness and completeness of the documentation was successful.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- records of the validation of the documentation
- raw & annotated scan results
- screenshots/logs of discovery attempts for logical interfaces

### 6.12.5 Assessment criteria for [LAS-SBOOT]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [LAS-SBOOT]
- a functional sufficiency assessment of the bootloader function used by the personal wearable to fulfil [LAS-SBOOT]

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- list of the personal wearable's hardware architectural component including information on which software's integrity and authenticity is protected by the bootloader function
- documentation on how the bootloader function verifies the integrity and authenticity of the hardware architectural component's software

The following test setup shall be prepared:

- a test setup for installing integrity and authenticity tampered core software, including a software package including the tampered core software; or
- a test setup for tampering the integrity of installed core software;

**Assessment activities:**

- The personal wearable's conformity to [LAS-SBOOT] shall be validated based on the documentation.
- The correct implementation of the bootloader function's integrity and authenticity verification of core software shall be verified based on:
  - tampering the integrity and authenticity of installed core software or installing integrity and authenticity tampered core software; and
  - restarting the personal wearable's hardware architectural component

NOTE: Typical results are:

- the bootloader function refuses to execute the tampered core software (and thus does not execute application software); and
- either halts, resets or boots into a secure fallback; and
- an error indication is provided (e.g. via a log, an error code, an LED pattern, etc.).

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the documentation indicates the personal wearable's conformity to [LAS-SBOOT]; and
- the personal wearable's hardware architectural component does not execute the modified core software.

Otherwise, the verdict FAIL shall be assigned.

**Assessment evidence:**

- records of the validation of the documentation
- descriptions of the performed tests and documentation of associated test records that verify the correct implementation of the bootloader function's integrity and authenticity verification

# 6.13 Exploit mitigation

## 6.13.1 Assessment criteria for [PRIV-DATA-HIGH]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [PRIV-DATA-HIGH];
- a functional sufficiency assessment of the personal wearable's mechanisms that ensure conformity with [PRIV-DATA-HIGH].

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- a list of the personal wearable's architectural components
- for each personal wearable's architectural component:
  - a list of processed data assets that are:
    - confidential data with [IMP.CONF.High]; or
    - integrity relevant data with [IMP.INT.High]; and
  - a description of the processes running on the same hardware as the architectural component that have privileges to access the listed data assets, including a justification for the necessity for the personal wearable's intended purpose.
  - a description of the mechanisms that ensure conformity with [PRIV-DATA-HIGH].

The following test setups shall be prepared:

- for each architectural component, a test setup for accessing confidential data with [IMP.CONF.High] and integrity relevant data with [IMP.INT.High] via unauthorized processes running on the same hardware.

**Assessment activities:**

- The personal wearable's conformity to [PRIV-DATA-HIGH] shall be validated based on the documentation.
- For each architectural component, the correct implementation the mechanisms that ensure conformity with [PRIV-DATA-HIGH] shall be verified by:
  - trying to access confidential data with [IMP.CONF.High] or integrity relevant data with [IMP.INT.High] via unauthorized processes.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the documentation indicates the personal wearable's conformity to [PRIV-DATA-HIGH]; and
- the verification of the correct implementation of the mechanisms that ensure conformity with [PRIV-DATA-HIGH] was successful.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation the mechanisms that ensure conformity with [PRIV-DATA-HIGH].

### 6.13.2 Assessment criteria for [PRIV-FUNC-HIGH]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [PRIV-FUNC-HIGH];
- a functional sufficiency assessment of the personal wearable's mechanisms that ensure conformity with [PRIV-FUNC-HIGH].

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- a list of the personal wearable's architectural components
- for each personal wearable's architectural component:
  - a list of provided function assets that are:
    - time sensitive function of [IMP.AVAI.TIME.High];
    - integrity relevant function of [IMP.INT.High]; or
    - function, whose use can cause harm of [IMP.FH.High];
  - a description of the processes running on the same hardware as the architectural component that have privileges to access the listed function assets, including a justification for the necessity for the personal wearable's intended purpose;
  - a description of the mechanisms that ensure conformity with [PRIV-FUNC-HIGH].

The following test setups shall be prepared:

- for each architectural component, a test setup for accessing time sensitive function with [IMP.AVAI.TIME.High], integrity relevant function with [IMP.INT.High] function, whose use can cause harm and [IMP.FH.High] via unauthorized processes running on the same hardware.

**Assessment activities:**

- The personal wearable's conformity to [PRIV-FUNC-HIGH] shall be validated based on the documentation.
- For each architectural component, the correct implementation the mechanisms that ensure conformity with [PRIV-FUNC-HIGH] shall be verified by:
  - trying to access time sensitive function with [IMP.AVAI.TIME.High], integrity relevant function with [IMP.INT.High] function, whose use can cause harm or [IMP.FH.High] via unauthorized processes.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the documentation indicates the personal wearable's conformity to [PRIV-FUNC-HIGH]; and
- the verification of the correct implementation of the mechanisms that ensure conformity with [PRIV-FUNC-HIGH] was successful.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation the mechanisms that ensure conformity with [PRIV-FUNC-HIGH].

## 6.14 Monitoring

### 6.14.1 Assessment criteria for [MON-LOW]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [MON-LOW]
- a functional sufficiency assessment of monitoring mechanisms used by the personal wearable to fulfil [MON-LOW]

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- list of all monitoring mechanisms
- documentation on how the monitoring mechanisms creates audit event data
- documentation which audit event data are created by which monitoring mechanism

The following test setups shall be prepared:

- a test user with the necessary permissions has been set up to trigger the events listed in [MON-LOW]
- monitoring mechanism are enabled on the personal wearable such that at least all the events in [MON-LOW] are covered
- a test setup for triggering the events listed in [MON-LOW]

**Assessment activities:**

The following activities shall be performed:

- Verify whether the *list of all monitoring mechanisms* is complete
- trigger the events listed in *Assessment preparation*:
  - for each event triggered: verify that audit event data is created according to the documentation

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the *list of all monitoring mechanisms* is complete; and
- for each event listed in *Assessment preparation* that could be triggered, audit event data is created.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- descriptions of the performed tests and records of performed tests

### 6.14.2 Assessment criteria for [MON-MEDIUM]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [MON-MEDIUM]
- a functional sufficiency assessment of monitoring mechanisms used by the personal wearable to fulfil [MON-MEDIUM]

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- list of all monitoring mechanisms
- documentation on how the monitoring mechanisms creates audit event data
- documentation which audit event data are created by which monitoring mechanism

The following test setups shall be prepared:

- a test user with the necessary permissions has been set up to trigger the events listed in [MON-MEDIUM]
- a test setup for triggering the events listed in [MON-MEDIUM]

**Assessment activities:**

The following activities shall be performed:

- Verify whether the *list of all monitoring mechanisms* is complete
- trigger the events listed in *Assessment preparation:*
  - for each event triggered: verify that audit event data is created according to the documentation

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the *list of all monitoring mechanisms* is complete; and
- for each event listed in *Assessment preparation* that could be triggered, audit event data is created.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- descriptions of the performed tests and records of performed tests

### 6.14.3 Assessment criteria for [MON-HIGH]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [MON-HIGH]

- a functional sufficiency assessment of monitoring mechanisms used by the personal wearable to fulfil [MON-HIGH]

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- list of all monitoring mechanisms
- documentation on how the monitoring mechanisms creates audit event data
- documentation which audit event data are created by which monitoring mechanism

The following test setups shall be prepared:

- a test user with the necessary permissions has been set up to trigger the events listed in [MON-HIGH]
- a test setup for triggering the events listed in [MON-HIGH]

**Assessment activities:**

The following activities shall be performed:

- Verify whether the *list of all monitoring mechanisms* is complete
- trigger the events listed in *Assessment preparation*:
    - for each event triggered: verify that audit event data is created according to the documentation

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the *list of all monitoring mechanisms* is complete; and
- for each event listed in *Assessment preparation* that could be triggered, audit event data is created.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- descriptions of the performed tests and records of performed tests

### 6.14.4 Assessment criteria for [MON-HANDLE]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of each audit event data generated by a monitoring mechanism of the personal wearable to fulfil [MON-HANDLE]

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

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

The following test setups shall be prepared:

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

**Assessment activities:**

The following activities shall be performed:

- For each audit event data listed in *assessment preparation* with assigned logging mechanism:
  - Verify that the assigned logging mechanism is enabled;
  - generate audit event data; and
  - check that the logging data produced by the logging mechanism from the audit event data is generated and stored.
- For each audit event data listed in *assessment preparation* with assigned data transfer mechanism:
  - check that the corresponding architectural component does not support public communication;
  - verify that the assigned data transfer mechanism is enabled;
  - generate audit event data; and
  - check that the audit event data is transferred to the destination (architectural component or other device).

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the documentation indicates the personal wearable's conformity with [MON-HANDLE];
- for every audit event data assigned to a logging mechanism corresponding logging data is generated and stored; and
- for every audit event data assigned to a data transfer mechanism:
  - the corresponding architectural component does not support public communication; and
  - audit event data is transferred to the destination.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- descriptions of the performed tests and records of performed tests

### 6.14.5 Assessment criteria for [LOG-TIME]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of logging mechanisms used by the personal wearable to fulfil [LOG-TIME]

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- documentation on how the logging mechanisms creates logging data
- documentation for which events logging data are created by which logging mechanism
- documentation on where logging data are stored
- documentation on the time sources and formats used by logging mechanism

The following test setups shall be prepared:

- a test user with the necessary permissions has been set up to trigger the events
- logging mechanism are enabled on the personal wearable such that at least all the events in the following point are covered
- a test setup for triggering events as described in *Assessment preparation* in clause 6.14.1 or clause 6.14.2

**Assessment activities:**

The following activities shall be performed:

- trigger the events listed in *Assessment preparation* and note the order and approximate time
  - for each event triggered: verify that the logging data contains a timestamp
- for all events triggered: verify that the order and relative times, in which the events where triggered, is represented by the logging data

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the *list of all logging mechanisms* is complete; and
- for each event listed in *Assessment preparation* that could be triggered, the logging data includes a timestamp; and
- the order and relative times, in which the events where triggered, is represented by the logging data.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- descriptions of the performed tests and records of performed tests

### 6.14.6 Assessment criteria for [LOG-TIME-HIGH]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [LOG-TIME-HIGH]
- a functional sufficiency assessment of logging mechanisms used by the personal wearable to fulfil [LOG-TIME-HIGH]

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- documentation on how the logging mechanisms creates logging data
- documentation for which events logging data are created by which logging mechanism
- documentation on where logging data are stored
- documentation on the time sources and formats used by logging mechanism

The following test setups shall be prepared:

- a test user with the necessary permissions has been set up to trigger the events
- logging mechanism are enabled on the personal wearable such that at least all the events in the following point are covered
- a test setup for triggering events as described in *Assessment preparation* in clause 6.14.3

**Assessment activities:**

The following activities shall be performed:

- Verify whether the documented time sources are able to produce real time data
- trigger the events listed in *Assessment preparation* and note the time:
    - for each event triggered: verify that the logging data contains a timestamp which represents the time, the event was triggered

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the *list of all logging mechanisms* is complete; and
- for each event listed in *Assessment preparation* that could be triggered, the logging data includes a timestamp which represents the time, the event was triggered

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- descriptions of the performed tests and records of performed tests

### 6.14.7 Assessment criteria for [LOG-STORE-MEDIUM]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of logging mechanisms used by the personal wearable to fulfil [LOG-STORE-MEDIUM]

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- list of all audit event data and for each entry:
    - documentation on which logging mechanism is used to generate and store corresponding logging data;
    - documentation on how the corresponding logging mechanism generates logging data; and

- documentation on where logging data are stored;
- documentation and reasoning on how many entries of this architectural component can be stored.

The following test setups shall be prepared:

- a test user with the necessary permissions has been set up to trigger the generation of audit event data
- logging mechanisms are enabled on the personal wearable such that at least all the events listed in [LOG-STORE-MEDIUM] (clause 5.14.2) are covered
- a test setup for triggering the generation of audit event data as described in *Assessment preparation* in [LOG-STORE-MEDIUM] (clause 6.14.2)

**Assessment activities:**

The following activities shall be performed:

- For each audit event data listed in *Assessment preparation*:
  - verify the reasoning for the number of stored entries of this architectural component;
  - trigger the generation of the audit event data;
  - trigger the generation of further audit event data for the same architectural component to reach the value before deletion or rotation as documented in *assessment preparation*; and
  - verify whether the logging data associated with the first audit event data is still present or a user notification informed about deletion or rotation.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- for each audit event data listed in *Assessment preparation* that could be used by logging mechanisms:
  - the reasoning for the number of stored entries of this architectural component is verified, and:
    - the logging data is still present after generation of further audit event data: or
    - user notification informed about deletion or rotation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- descriptions of the performed tests and records of performed tests

## 6.14.8 Assessment criteria for [LOG-STORE-HIGH]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of logging mechanisms used by the personal wearable to fulfil [LOG-STORE-HIGH]

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- list of all audit event data and for each entry:
  - documentation on which logging mechanism is used to generate and store corresponding logging data;

- documentation on how the corresponding logging mechanism generates logging data; and
- documentation on where logging data are stored;
- documentation and reasoning on how many entries of this architectural component can be stored.

The following test setups shall be prepared:

- a test user with the necessary permissions has been set up to trigger the generation of audit event data
- logging mechanisms are enabled on the personal wearable such that at least all the events listed in [LOG-STORE-HIGH] (clause 5.14.3) are covered
- a test setup for triggering the generation of audit event data as described in *Assessment preparation* in [LOG-STORE-HIGH] (clause 6.14.3)

**Assessment activities:**

The following activities shall be performed:

- For each audit event data listed in *Assessment preparation*:
  - verify the reasoning for the number of stored entries of this architectural component;
  - trigger the generation of the audit event data;
  - trigger the generation of further audit event data for the same architectural component to reach the value before deletion or rotation as documented in *assessment preparation*; and
  - verify whether the logging data associated with the first audit event data is still present or a user notification informed about deletion or rotation.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- for each audit event data listed in *Assessment preparation* that could be used by logging mechanisms,
  - the reasoning for the number of stored entries of this architectural component is verified, and
    - the logging data is still present after generation of further audit event data, or
    - user notification informed about deletion or rotation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- descriptions of the performed tests and records of performed tests

### 6.14.9 Assessment criteria for [LOG-CONFIG]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [LOG-CONFIG];
- a functional sufficiency assessment of each logging mechanism used by the personal wearable to fulfil [LOG-CONFIG];

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- a description of each logging mechanism, including:
  - which audit event data can be processed
  - which logging data are generated
  - where the generated logging data is stored
  - where and how to disable the {SupportingFunctionality:LoggingMechanism}; or
  - the evidence that the disabling mechanism is not supported for security reasons.

The following test setups shall be prepared for each logging mechanism supporting the user disabling:

- a test setup that allows to identify logging mechanisms on a sample personal wearable in default configuration;
- for each logging mechanism, a test setup that allows to:
  - generate audit event data
  - access the storage location where logging data is stored
  - see the user interaction steps (e.g. menu, dialog, confirmation after deletion)

**Assessment activities:**

The following activities shall be performed for each logging mechanism supporting the user disabling:

- The personal wearable's conformity to [LOG-CONFIG] shall be validated based on the documentation.
- The correctness of the documentation shall be verified by checking that all documented logging mechanisms have an option to be disabled.
  - For each logging mechanism, its possibility to be disabled shall be verified by:
    - generating audit event data;
    - check that corresponding logging data is generated (and stored) by the logging mechanism;
    - disable the logging mechanism as documented; and
    - check that generating audit event data no longer leads to logging data generated (and stored) by the logging mechanism.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the documentation indicates the personal wearable's conformity with [LOG-CONFIG]; and
- the verification of the correctness of the documentation was successful; and
- all logging mechanisms supporting the user disabling have a possibility to be disabled.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

# 6.15 Factory reset and data portability

## 6.15.1 Assessment criteria for [DLM-PERM]

**Assessment objective:**

The assessment covers:

- a conceptual assessment of [DLM-PERM];
- a functional completeness assessment on the personal wearable's capabilities that are addressed by [DLM-PERM]; and
- a functional sufficiency assessment of each deletion mechanism used by the personal wearable to fulfil [DLM-PERM];

based on the default configuration required by clause 5.4.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- a description of each deletion mechanism, including:
  - deletion scope (i.e. describing what can be deleted by this mechanism);
  - method of deletion (e.g. overwriting, access control, changing pointer address, etc.);
  - method of user interaction and initiation steps;
  - whether confirmation is provided after deletion is performed;
  - multi-user handling (describing the user rights to delete other users' data).

The following test setups shall be prepared:

- a test setup that allows to identify deletion mechanisms on a sample personal wearable in default configuration;
- for each deletion mechanism, a test setup that allows to:
  - create representative user-related data and install applications;
  - access the storage location where data and applications are stored; and
  - see the user interaction steps (e.g. menu, dialog, confirmation after deletion).

**Assessment activities:**

The following activities shall be performed:

- The personal wearable's conformity to [DLM-PERM] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by checking that all documented deletion mechanisms are implemented:
  - For each deletion mechanism, its correct implementation shall be verified by:
    - generating user-related data and installing an application as a user,
    - deleting the generated user-related data and the application and
    - checking whether the:
      - user-related data and the application are permanently removed, e.g. by at least checking the storage location of the user-related data and application before and after deletion;

  - deletion mechanism is easy to use with limited technical knowledge;
  - user can only delete its own data in multi-user systems; and
  - user is provided with clear confirmation of deletion after user-related data or a user-installed application have been deleted.

- Over all deletion mechanisms, it is to be checked whether all generated sample user-related data and installed applications can be permanently removed.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the documentation indicates the personal wearable's conformity with [DLM-PERM]; and
- the verification of the correctness and completeness of the documentation was successful; and
- the verification of the correct implementation of each deletion mechanism was successful; and
- all deletion mechanisms are able to permanently remove all generated user-related data and user-installed applications.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- records of the validation of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correctness and completeness of the documentation;
- descriptions of the performed tests and records of performed tests to verify the correct implementation of each update mechanism and the ability of the personal wearable to delete all generated user-related data and applications.

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

The present document has been prepared under the Commission's Standardisation request M/606 - C(2025)618 [i.3] to provide one voluntary means of conforming to the requirements of Regulation (EU) No 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) [i.1].

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

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

| Description | Essential Requirements of Regulation (EU) 2024/2847 | Clause(s) of the present document | Remarks / Notes |
|---|---|---|---|
| Annex I, Part I, (1) | The design, development, and production of products with digital elements ensures an appropriate level of cybersecurity based on the risks. | [ACM-FH] 5.6.1; 6.6.1<br>[AUM-FH] 5.6.2; 6.6.2<br>[AUTHZ-LP] 5.6.3; 6.6.3<br>[AUTHZ-R] 5.6.4; 6.6.4<br>[AUTHZ-PC] 5.6.6; 6.6.6<br>[AVAI-TIME-RECO-POW] 5.10.1; 6.10.1<br>[AVAI-TIME-NETW] 5.10.2; 6.10.2<br>[AVAI-TIME-RECO-NETW] 5.10.3; 6.10.3<br>[AVAI-TIME-OUTA-NOT] 5.10.4; 6.10.4<br>[AVAI-TIME-PREV-NOT] 5.10.5; 6.10.5<br>[AVAI-TIME-PREV-PRIO] 5.10.6; 6.10.6<br>[AVAI-TIME-RES-PRIO] 5.10.7; 6.10.7<br>[AVAI-SUM-SCHEDULE] 5.10.8; 6.10.8<br>[BACKUP-TRANS] 5.4.2; 6.4.2<br>[BACKUP-AUTOTRANS] 5.2.5; 6.2.5<br>[BACKUP-EXPORT] 5.2.6; 6.2.6<br>[CONF-SSM] 5.7.1; 6.7.1<br>[CONF-COM] 5.7.2; 6.7.2<br>[CONF-MON-HW] 5.7.3; 6.7.3<br>[CRY-SOTA] 5.4.7; 6.4.7<br>[CRY-CCK-PRE-LEN] 5.4.8; 6.4.8<br>[CRY-CCK-GEN] 5.4.9; 6.4.9<br>[CRY-PW-PRE-COM] 5.4.10; 6.4.10<br>[CRY-PW-GEN-COM] 5.4.11; 6.4.11<br>[CRY-PW-USR-COM] 5.4.12; 6.4.12<br>[DLM-PERM] 5.15.1; 6.15.1<br>[DMIN-DJST] 5.9.1; 6.9.1<br>[PRIV-DATA-HIGH] 5.13.1; | |

| Description | Essential Requirements of Regulation (EU) 2024/2847 | Clause(s) of the present document | Remarks / Notes |
|---|---|---|---|
| | | 6.13.1<br>[PRIV-FUNC-HIGH] 5.13.2; 6.13.2<br>[INT-SSM] 5.8.1; 6.8.1<br>[INT-COM] 5.8.3; 6.8.3<br>[INT-SWPCK] 5.8.2; 6.8.2<br>[LAS-INVAL] 5.12.1; 6.12.1<br>[LAS-INSAN] 5.12.2; 6.12.2<br>[LAS-PHY-INF] 5.12.3; 6.12.3<br>[LAS-LOGIC-INF] 5.12.4; 6.12.4<br>[LAS-SBOOT] 5.12.5; 6.12.5<br>[MON-LOW] 5.14.1; 6.14.1<br>[MON-MEDIUM] 5.14.2; 6.14.2<br>[MON-HIGH] 5.14.3; 6.14.3<br>[MON-HANDLE] 5.14.4; 6.14.4<br>[LOG-TIME] 5.14.5; 6.14.5<br>[LOG-TIME-HIGH] 5.14.6; 6.14.6<br>[LOG-STORE-MEDIUM] 5.14.7; 6.14.7<br>[LOG-STORE-HIGH] 5.14.8; 6.14.8<br>[LOG-CONFIG] 5.14.9; 6.14.9<br>[NKEV-MKAV] 5.3.1; 6.3.1<br>[NKEV-INIT-UPD] 5.3.2; 6.3.2<br>[PARCONT] 5.6.5; 6.6.5<br>[SDC-AUM-FH] 5.4.1; 6.4.1<br>[SDC-SUM-AUTO] 5.4.2; 6.4.2<br>[SDC-SUM-NOTIF] 5.4.3; 6.4.3<br>[SDC-FRM] 5.4.4; 6.4.4<br>[SDC-PARCONT] 5.4.5; 6.4.5<br>[SDC-MON-HANDLE] 5.4.6; 6.4.6<br>[SU-SUPPORT] 5.5.1; 6.5.1<br>[SU-PROVIDE] 5.5.2; 6.5.2<br>[SU-AUTO] 5.5.3; 6.5.3<br>[SU-DISABLE-AUTO] 5.5.4; 6.5.4<br>[SU-POSTPONE-AUTO] 5.5.5; 6.5.5<br>[SU-NOTIF] 5.5.6; 6.5.6<br>[USERNOT-NOSECFUC] 5.2.1; 6.2.1<br>[USERNOT-SECREL] 5.2.2; 6.2.2<br>[GUI-SECCONF] 5.2.3; 6.2.3 | |

| Description | Essential Requirements of Regulation (EU) 2024/2847 | Clause(s) of the present document | Remarks / Notes |
|---|---|---|---|
| Annex I, Part I, (2)(a) | Products with digital elements are made available on the market without known exploitable vulnerabilities. | [NKEV-MKAV] 5.3.1; 6.3.1<br>[NKEV-INIT-UPD] 5.3.2; 6.3.2 | |
| Annex I, Part I, (2)(b) | 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. | [CRY-SOTA] 5.4.7; 6.4.7<br>[CRY-CCK-PRE-LEN] 5.4.8; 6.4.8<br>[CRY-CCK-GEN] 5.4.9; 6.4.9<br>[CRY-PW-PRE-COM] 5.4.10; 6.4.10<br>[CRY-PW-GEN-COM] 5.4.11; 6.4.11<br>[CRY-PW-USR-COM] 5.4.12; 6.4.12<br>[LAS-LOGIC-INF] 5.12.4; 6.12.4<br>[SDC-AUM-FH] 5.4.1; 6.4.1<br>[SDC-SUM-AUTO] 5.4.2; 6.4.2<br>[SDC-SUM-NOTIF] 5.4.3; 6.4.3<br>[SDC-FRM] 5.4.4; 6.4.4<br>[SDC-PARCONT] ] 5.4.5; 6.4.5<br>[SDC-MON-HANDLE] 5.4.6; 6.4.6 | |
| Annex I, Part I, (2)(c) | 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. | [SDC-SUM-AUTO] 5.4.2; 6.4.2<br>[SDC-SUM-NOTIF] 5.4.3; 6.4.3<br>[SU-SUPPORT] 5.5.1; 6.5.1<br>[SU-PROVIDE] 5.5.2; 6.5.2<br>[SU-AUTO] 5.5.3; 6.5.3<br>[SU-DISABLE-AUTO] 5.5.4; 6.5.4<br>[SU-POSTPONE-AUTO] 5.5.5; 6.5.5<br>[SU-NOTIF] 5.5.6; 6.5.6 | |
| Annex I, Part I, (2)(d) | Products with digital elements ensure protection from Unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible Unauthorised access. | [ACM-FH] 5.6.1; 6.6.1<br>[AUM-FH] 5.6.2; 6.6.2<br>[AUTHZ-LP] 5.6.3; 6.6.3<br>[AUTHZ-R] 5.6.4; 6.6.4<br>[AUTHZ-PC] 5.6.6; 6.6.6<br>[MON-MEDIUM] 5.14.2; 6.14.2<br>[MON-HIGH] 5.14.3; 6.14.3<br>[LOG-TIME] 5.14.5; 6.14.5<br>[LOG-TIME-HIGH] 5.14.6; 6.14.6<br>[PARCONT] 5.6.5; 6.6.5<br>[SDC-AUM-FH] 5.4.1; 6.4.1 | |
| Annex I, Part I, (2)(e) | 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. | [ACM-FH] 5.6.1; 6.6.1<br>[AUM-FH] 5.6.2; 6.6.2<br>[AUTHZ-LP] 5.6.3; 6.6.3<br>[AUTHZ-R] 5.6.4; 6.6.4<br>[AUTHZ-PC] 5.6.6; 6.6.6<br>[CONF-SSM] 5.7.1; 6.7.1<br>[CONF-COM] 5.7.2; 6.7.2<br>[CONF-MON-HW] 5.7.3; 6.7.3 | |

| Description | Essential Requirements of Regulation (EU) 2024/2847 | Clause(s) of the present document | Remarks / Notes |
|---|---|---|---|
| Annex I, Part I, (2)(f) | Products with digital elements protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions. | [ACM-FH] 5.6.1; 6.6.1<br>[AUM-FH] 5.6.2; 6.6.2<br>[AUTHZ-LP] 5.6.3; 6.6.3<br>[AUTHZ-R] 5.6.4; 6.6.4<br>[AUTHZ-PC] 5.6.6; 6.6.6<br>[INT-SSM] 5.8.1; 6.8.1<br>[INT-COM] 5.8.3; 6.8.3<br>[INT-SWPCK] 5.8.2; 6.8.2<br>[MON-LOW] 5.14.1; 6.14.1<br>[MON-MEDIUM] 5.14.2; 6.14.2<br>[MON-HIGH] 5.14.3; 6.14.3 | |
| Annex I, Part I, (2)(g) | Products with digital elements process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation). | [DMIN-DJST] 5.9.1; 6.9.1 | |
| Annex I, Part I, (2)(h) | 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. | [AVAI-TIME-RECO-POW] 5.10.1; 6.10.1<br>[AVAI-TIME-NETW] 5.10.2; 6.10.2<br>[AVAI-TIME-RECO-NETW] 5.10.3; 6.10.3<br>[AVAI-TIME-OUTA-NOT] 5.10.4; 6.10.4<br>[AVAI-TIME-PREV-NOT] 5.10.5; 6.10.5<br>[AVAI-TIME-PREV-PRIO] 5.10.6; 6.10.6<br>[AVAI-TIME-RES-PRIO] 5.10.7; 6.10.7<br>[AVAI-SUM-SCHEDULE] 5.10.8; 6.10.8 | Specific mitigation measures against denial-of-service attacks are not addressed by the present document because personal wearable are not reachable over the internet (they do not have their own IP address) and does not allow incoming connection as server. Personal Wearable RDPS relies on the DOS mitigation measures of the hosting gateway or cloud. |
| Annex I, Part I, (2)(i) | Products with digital elements minimise the negative impact by the products themselves or connected products on the availability of services provided by other products or networks. | [ACM-FH] 5.6.1; 6.6.1<br>[AUM-FH] 5.6.2; 6.6.2<br>[AUTHZ-LP] 5.6.3; 6.6.3<br>[AUTHZ-R] 5.6.4; 6.6.4<br>[AUTHZ-PC] 5.6.6; 6.6.6<br>[INT-SWPCK] 5.8.2; 6.8.2<br>[LAS-SBOOT] 5.12.5; 6.12.5 | |
| Annex I, Part I, (2)(j) | Products with digital elements are designed, developed and produced to limit attack surfaces, including external interfaces. | [LAS-INVAL] 5.12.1; 6.12.1<br>[LAS-INSAN] 5.12.2; 6.12.2<br>[LAS-PHY-INF] 5.12.3; 6.12.3<br>[LAS-LOGIC-INF] 5.12.4; 6.12.4<br>[LAS-SBOOT] 5.12.5; 6.12.5 | |
| Annex I, Part I, (2)(k) | Products with digital elements are designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques. | [AVAI-TIME-RECO-POW] 5.10.1; 6.10.1<br>[AVAI-TIME-RES-PRIO] 5.10.7; 6.10.7<br>[PRIV-DATA-HIGH] 5.13.1; 6.13.1<br>[PRIV-FUNC-HIGH] 5.13.2; 6.13.2 | |

| Description | Essential Requirements of Regulation (EU) 2024/2847 | Clause(s) of the present document | Remarks / Notes |
|---|---|---|---|
| Annex I, Part I, (2)(l) | 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. | [MON-LOW] 5.14.1; 6.14.1<br>[MON-MEDIUM] 5.14.2; 6.14.2<br>[MON-HIGH] 5.14.3; 6.14.3<br>[MON-HANDLE] 5.14.4; 6.14.4<br>[LOG-TIME] 5.14.5; 6.14.5<br>[LOG-TIME-HIGH] 5.14.6; 6.14.6<br>[LOG-STORE-MEDIUM] 5.14.7; 6.14.7<br>[LOG-STORE-HIGH] 5.14.8; 6.14.8<br>[LOG-CONFIG] 5.14.9; 6.14.9<br>[SDC-MON-HANDLE] 5.4.6; 6.4.6<br>[SU-DISABLE-AUTO] 5.5.4; 6.5.4<br>[SU-POSTPONE-AUTO] 5.5.5; 6.5.5<br>[SU-NOTIF] 5.5.6; 6.5.6<br>[USERNOT-NOSECFUC] 5.2.1; 6.2.1 | |
| Annex I, Part I, (2)(m) | 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. | [DLM-PERM] 5.15.1; 6.15.1<br>[SDC-FRM] 5.4.4; 6.4.4 | |

**Key to columns:**

**Description** A textual reference to the requirement.

**Requirements of Regulation**

Identification of point(s) defining the requirement in Regulation (EU) 2024/2847 - the Cyber Resilience Act.

**Clause(s) of the present document**

Identification of clause(s) addressing the requirement in the present document

Presumption of conformity stays valid only as long as a reference to the present document is maintained in the list published in the Official Journal of the European Union. Users of the present document should consult frequently the latest list published in the Official Journal of the European Union.

Other Union legislation may be applicable to the product(s) falling within the scope of the present document.

# Annex B (informative): Security analysis

## B.1 General

This annex documents the security analysis on which the present document bases on.

This annex applies state of the art methodology to identify assets, threats, identify and evaluate risk factors.

## B.2 Assets

The present document uses the categories data assets and function assets to classify the different assets. Different items of those asset categories are typically interlinked, e.g. in general:

- function assets can create, modify, use, delete, communicate or otherwise process data assets;
- function assets can trigger other function assets;
- data assets can control function assets; and
- executable code that implements function assets is a data asset (here function binary data).

The function assets addressed by the present document are listed in clause 4.1.7.

The data assets addressed by the present document are listed in clause 4.1.8.

## B.3 Risk factors

The present document uses the categories impact and attack surface to classify the risk factors.

The attack surface parameter used by the present document are:

- physical operational environment - [POE], where details are described in clause 4.3.2;
- logical operational environment - [LOE] expressed in terms of possible communication types - [COM], where details are described in clause 4.3.3;
- interface - [IF], where details are described in clause 4.3.4;
- users, where details are described in clause 4.5.

The impact parameter used by the present document are:

- impact classes - [IMP] assigned to the data assets and function asset provided in clauses 4.1.7 and 4.1.8. The impact class assignment is provided in Annex D.

Those risk factors are used to determine the applicability of the technical requirements and their corresponding details.

## B.4 Assumptions

The present document assumes that personal wearable are used according to their intended purpose and reasonably foreseeable use.

## B.5 Threats

The present document addresses the threats scenarios described by the columns *Threat Actor*, *Threat Action*, *Asset*, and *Threat Details* of Table B.1.

## B.6 Relationship between the present document and the covered/not covered cybersecurity risks

Table B.1 amends the threat scenarios considered by the related risk factors, corresponding mitigation measures and a statement on the acceptability of residual risk.

**Table B.1: Covered threats and remaining risks acceptance**

| No. | Threat Actor | Threat action | Asset (relevant impact parameter) | Threat details | | Requirement(s) for mitigation | Relevant attack surface parameter | Risk coverage |
|---|---|---|---|---|---|---|---|---|
| **[1]** | A threat actor | (mis)uses | a function whose use can cause harm | on the personal wearable | | **Prevention**:<br>[ACM-FH]<br>[AUM-FH]<br>[AUTHZ-LP]<br>[AUTHZ-R]<br>[PRIV-FUNC-HIGH]<br>[LAS-PHY-INF]<br>[LAS-LOGIC-INF<br>[SDC-AUM-FH]<br>**Information**:<br>[MON-LOW]<br>[MON-MEDIUM]<br>[MON-HIGH]<br>[MON-HANDLE]<br>[LOG-TIME]<br>[LOG-TIME-HIGH]<br>[LOG-STORE-MEDIUM]<br>[LOG-STORE-HIGH]<br>[LOG-CONFIG]<br>[USERNOT-NOSECFUC]<br>**Restoration**:<br>[SDC-FRM] | COM, IF and POE | C |
| **[2]** | A threat actor | tampers | integrity relevant data | permanently stored on the personal wearable | | **Prevention**:<br>[PRIV-DATA-HIGH]<br>[INT-SSM] | | C |
| **[3]** | A threat actor | tampers | integrity relevant data | volatile stored on the personal wearable | | **Prevention**:<br>[PRIV-DATA-HIGH] | | C |
| **[4]** | A threat actor | tampers | integrity relevant data | communicated from or to the architectural component | | **Prevention**:<br>[INT-COM] | COM, IF and POE | C |
| **[5]** | A threat actor | discloses | confidential data | on the personal wearable | unnecessarily processed | **Prevention**:<br>[DMIN-DJST]<br>**Information**:<br>[CONF-MON-HW] | | C |
| **[6]** | A threat actor | discloses | confidential data | permanently stored on the personal wearable | during storage | **Prevention**:<br>[CONF-SSM]<br>[PRIV-DATA-HIGH] | POE | C |
| **[7]** | A threat actor | discloses | confidential data | permanently stored on the personal wearable | after deletion | **Prevention**:<br>[DLM-PERM] | | C |

| No. | Threat Actor | Threat action | Asset (relevant impact parameter) | Threat details | | Requirement(s) for mitigation | Relevant attack surface parameter | Risk coverage |
|---|---|---|---|---|---|---|---|---|
| **[8]** | A threat actor | discloses | confidential data | volatile stored on the personal wearable | during usage | **Prevention**:<br>[PRIV-DATA-HIGH] | | C |
| **[9]** | A threat actor | discloses | confidential data | volatile stored on the personal wearable | after usage | **Prevention**:<br>[PRIV-DATA-HIGH] | | C |
| **[10]** | A threat actor | discloses | confidential data | communicated from or to the architectural component | | **Prevention**:<br>[CONF-COM]<br>[DMIN-LOCAL] | COM, IF and POE | C |
| **[12]** | A threat actor | tampers | integrity relevant function | on the personal wearable | | **Prevention**:<br>[PRIV-DATA-HIGH]<br>[PRIV-FUNC-HIGH]<br>[INT-SWPCK]<br>[LAS-SBOOT] | | C |
| **[13]** | A threat actor | impacts the availability of | time sensitive function | on the personal wearable | by interruption caused by a software update installation | **Prevention**:<br>[AVAI-SUM-SCHEDULE] | | C |
| **[14]** | A threat actor | impacts the availability of | time sensitive function | on the personal wearable | by interruption of power supply | **Information**:<br>AVAI-TIME-OUTA-NOT]<br>[AVAI-TIME-PREV-NOT]<br>**Restoration**:<br>[AVAI-TIME-RECO-POW] | | C |
| **[15]** | A threat actor | impacts the availability of | time sensitive function | on the personal wearable | by interruption of network connection | **Prevention**:<br>[AVAI-TIME-NETW]<br>**Information**:<br>[AVAI-TIME-OUTA-NOT]<br>[AVAI-TIME-PREV-NOT]<br>**Restoration**:<br>[AVAI-TIME-RECO-NETW] | | C |
| **[16]** | A threat actor | impacts the availability of | time sensitive function | on the personal wearable | due to overloading of a resource or connection | **Prevention**:<br>[AVAI-TIME-NET-PRIO]<br>[AVAI-TIME-RES-PRIO]<br>**Information**:<br>[AVAI-TIME-OUTA-NOT] | IF | C |

| No. | Threat Actor | Threat action | Asset (relevant impact parameter) | Threat details | | Requirement(s) for mitigation | Relevant attack surface parameter | Risk coverage |
|---|---|---|---|---|---|---|---|---|
| **[17]** | A threat actor | exploits an implementation vulnerability to compromise | a product cybersecurity asset | | | **Prevention**:<br>[PRIV-DATA-HIGH]<br>[PRIV-FUNC-HIGH]<br>[LAS-INVAL]<br>[LAS-INSAN]<br>[NKEV-MKAV]<br>**Information**:<br>[NKEV-INIT-UPD]<br>[SDC-SUM-NOTIF]<br>[SU-DISABLE-AUTO]<br>[SU-POSTPONE-AUTO]<br>[SU-NOTIF]<br>**Restoration**:<br>[NKEV-INIT-UPD]<br>[SDC-SUM-AUTO]<br>[SU-SUPPORT]<br>[SU-PROVIDE]<br>[SU-AUTO] | | C |
| **[18]** | A user | unconsciously performs an incorrect actions | | on the wearable | | **Prevention**:<br>[GUI-SECCONF]<br>**Information**:<br>[GUI-SECCONF] | IF.Human | C |
| **[19]** | A user | performs insecure actions | | on the personal wearable | because the user is not aware of security relevant information | **Prevention**:<br>[USERNOT-SECREL]<br>**Information**:<br>[USERNOT-SECREL] | IF.Human | C |
| **[20]** | A user | unknowingly creates confidential | audio or video capture data | on the personal wearable | | **Information**:<br>[CONF-MON-HW] | IF.Human | C |
| **[21]** | An incident | results in a permanent loss of | loss sensitive data | permanently stored on the personal wearable | | **Prevention**:<br>[BACKUP-TRANS]<br>[BACKUP-AUTOTRANS]<br>[BACKUP-EXPORT] | | C |

- The columns *Threat Actor*, *Threat Action*, *Asset*, and *Threat Details* describe the threat scenario under consideration.
- The column *Asset* describes the asset affected by this threat scenario and indicates, where relevant, the corresponding impact parameter (e.g. [IMP.FH] is the relevant impact parameter for threats addressing function, whose use can cause harm).
- The column *Requirement(s) for mitigation* refers to the mitigations of the risks that arise from the threat scenario.
- The *Relevant attack surface parameter* column describes which of the attack surface parameters make a difference in mitigation.
- The *Risk coverage* column describes whether the risk associated with the threat scenario has been reduced to an acceptable residual risk (C) or not (N).

# B.7 Guidance for determining impact classes

## B.7.1 General

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

## B.7.2 Confidential data

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

The disclosure may lead to:

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

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

The disclosure may lead to:

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

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

The disclosure may lead to:

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

## B.7.3 loss sensitive data

**loss sensitive availability impact class low (IMP.AVAI.LOSS.Low):**

The loss may lead to:

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

**loss sensitive availability impact class medium (IMP.AVAI.LOSS.Medium):**

The loss may lead to:

- serious impact on the user(s); or
- non-availability of essential functionalities of the personal wearable over a short time; or
- non-availability of essential functionalities on the personal wearable for a prolonged time.

**loss sensitive availability impact class high (IMP.AVAI.LOSS.High):**

The loss may lead to:

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

## B.7.4 time sensitive data and time sensitive function

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

The delay of availability may lead to:

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

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

The delay of availability may lead to:

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

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

The delay of availability may lead to:

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

## B.7.5 integrity relevant data and integrity relevant function

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

The tampering may lead to:

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

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

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

The tampering may lead to:

- serious impact on the user(s);
- additional or increased attack opportunities over a short time on the personal wearable; or a limited number of other personal wearables;
- additional or increased attack opportunities over a prolonged time limited to non-essential functionalities on the personal wearable; or
- non-availability of essential functionalities on the personal wearable for a short time; or
- non-availability of non-essential functionalities on the personal wearable for a prolonged time.

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

The tampering may lead to:

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

# Annex C:
# Void

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

## D.1 Data assets

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

| Specific data asset | Impact class for data asset categories | | | |
|---|---|---|---|---|
| | **Impact class for confidential personal wearable data** | **Impact class for integrity relevant personal wearable data** | **Impact class for time critical availability relevant personal wearable data** | **Impact class for loss critical availability relevant personal 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 |
| | | | | |
| | | | | |
| | | | | |
| audio data; | IMP.CONF.Low | NO | NO | NO |
| video data; | IMP.CONF.Low | NO | NO | NO |
| | | | | |
| | | | | |
| audio data (for children use); | IMP.CONF.Medium | IMP.INT.Low | IMP.AVAI.TIME.Low | IMP.AVAI.LOSS.Low |
| video 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 |

# D.2 Function assets

## D.2.1 Functions

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

| Specific function asset | Impact class for function asset categories | | |
|---|---|---|---|
| | Impact class for integrity relevant function | Impact class for time sensitive function | Impact class for function, whose use can cause harm |
| health monitoring functionalities | IMP.INT.Medium | IMP.AVAI.TIME.Medium | No |
| health monitoring functionalities (for babies care use) | IMP.INT.Medium | IMP.AVAI.TIME.Medium | IMP.FH.High |
| 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 |
| geofencing (for children use) | IMP.INT.High | IMP.AVAI.TIME.High | IMP.FH.High |
| parental control functionalities (for children use) | IMP.INT.High | IMP.AVAI.TIME.High | IMP.FH.High |
| 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 functionalities | IMP.INT.Low | IMP.AVAI.TIME.Low | No |
| audio functionalities (for children use) | IMP.INT.High | IMP.AVAI.TIME.Medium | IMP.FH.Low |
| video functionalities | IMP.INT.Low | IMP.AVAI.TIME.Low | No |
| video functionalities (for children use) | IMP.INT.High | IMP.AVAI.TIME.Medium | IMP.FH.Low |
| functionalities which can communicate personal 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) |

## D.2.2 Functions whose use can cause harm

The contents of the column *impact class for function, whose use can cause harm* of Table D.2 are split into details in Table D.3.

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

| Specific function asset | Impact class for function, 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 |
|---|---|---|---|---|
| health monitoring functionalities (for babies care use) | IMP.FH.SP.High | NO | IMP.FH.CCON = IMP.CONF of communicated control data | MP.FH.SP.Medium |
| 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 |
| geofencing (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 |
| | | | | |
| | | | | |
| notification functionalities | IMP.FH.SP = IMP.FH.SP of the function who generated the notification | NO | NO | NO |
| audio functionalities (for children use) | IMP.FH.SP.Low | NO | NO | NO |
| video functionalities (for children use) | IMP.FH.SP.Low | NO | NO | NO |
| functionalities which can communicate personal wearable data assets | NO | IMP.FH.DSN.Low | IMP.FH.CCON = IMP.CONF of communicated control data | NO |

# Annex E (normative): Protection measures

## E.1 authentication mechanism strength

### E.1.1 [AUM-FH] Authentication for functions whose use can cause harm

#### E.1.1.1 General

Specific requirements on authentication mechanisms for the AUTH strength level determined in clause 5.6.2. Note that for AUTH.Medium, AUTH.Enhanced and AUTH.Strong, the requirements in clause E.1.1.5 and clause E.1.1.6 are also to be considered.

#### E.1.1.2 [AUM-E-I-Basic] AUTH.Basic inherence based SFA

Where an authentication factor of the type inherence is used to achieve AUTH.Basic, the authentication mechanisms shall ensure a false acceptance rate of maximal $10^{-4}$ and a false rejection rate of maximal $10^{-1}$.

NOTE: The values used for false acceptance rate and false rejection rate are based on ETSI TS 103 732-2 [i.6].

#### E.1.1.3 [AUM-E-K-Basic] AUTH.Basic knowledge based SFA

Where an authentication factor of the type knowledge is used to achieve AUTH.Basic, the authentication mechanisms shall ensure a security insurance time of one day (86 400 seconds) with a probability of guessing a cryptographic parameter of maximal $10^{-2}$.

NOTE: The $p_{GRP}$ allows for a tradeoff between complexity of passwords or PINs and restrictions on the number of attempts to enter a password or PIN.

#### E.1.1.4 [AUM-E-I-Medium] AUTH.Medium inherence based SFA

Where an authentication factor of the type inherence is used to achieve AUTH.Medium, the authentication mechanisms shall ensure a false acceptance rate of maximal $5 * 10^{-5}$ and a false rejection rate of maximal $10^{-1}$.

NOTE: The values used for false acceptance rate and false rejection rate are based on ETSI TS 103 732-2 [i.6].

#### E.1.1.5 [AUM-E-K-Medium] AUTH.Medium knowledge based SFA

Where an authentication factor of the type knowledge is used to achieve AUTH.Medium, the authentication mechanisms shall ensure a security insurance time of one month ( $2{,}6 * 10^6$ seconds) with a probability of guessing a cryptographic parameter of maximal $10^{-3}$.

NOTE: The $p_{GRP}$ allows for a tradeoff between complexity of passwords or PINs and restrictions on the number of attempts to enter a password or PIN.

#### E.1.1.6 [AUM-E-P-Medium] AUTH.Medium possession based SFA

Where an account or service is used as a possession type authentication factor to achieve AUTH.Medium, the authentication mechanisms shall ensure that

- derived tokens have a time during which a token is valid of maximal 15 minutes (900 seconds) and

- all derived tokens than can be valid at the same time have a combined probability of guessing a cryptographic parameter of maximal $10^{-3}$ within the time during which a token is valid.

NOTE 1: The $p_{GRP}$ allows for a tradeoff between complexity of passwords or PINs and restrictions on the number of attempts to enter a password or PIN.

NOTE 2: The calculation of $L_{CP,eff}$ is based on the recommendations in [[@NIST-SP-800].

### E.1.1.7 [AUM-E-MFA-Medium] AUTH.Medium MFA

Where multiple authentication factors are used to achieve AUTH.Medium, the authentication mechanism shall ensure that:

- at least two authentication factors are of different types (inherence, knowledge or possession); and
- it fulfils the respective SFA requirements of at least AUTH.Basic with at least these two authentication factors; and
- that the authentication request is only considered valid if at least these two authentication factors are validated within maximal 30 minutes (1 800 seconds) of each other.

### E.1.1.8 [AUM-E-I-Enhanced] AUTH.Enhanced inherence based SFA

Where an authentication factor of the type inherence is used to achieve AUTH.Enhanced, the authentication mechanisms shall ensure a false acceptance rate of maximal $2 \times 10^{-5}$ and a false rejection rate of maximal $3 \times 10^{-2}$.

NOTE: The values used for false acceptance rate and false rejection rate are based on ETSI TS 103 732-2 [i.6] [i.6].

### E.1.1.9 [AUM-E-K-Enhanced] AUTH.Enhanced knowledge based SFA

Where an authentication factor of the type knowledge is used to achieve AUTH.Enhanced, the authentication mechanisms shall ensure a security insurance time of one year ($3.2 * 10^7$ seconds ) with a probability of guessing a cryptographic parameter of maximal $10^{-5}$.

NOTE: The $p_{GRP}$ allows for a tradeoff between complexity of passwords or PINs and restrictions on the number of attempts to enter a password or PIN.

### E.1.1.10 [AUM-E-P-Enhanced] AUTH.Enhanced possession based SFA

Where an account or service or security token is used as a possession type authentication factor to achieve AUTH.Enhanced, the authentication mechanisms shall ensure that

- confidential cryptographic keys in security tokens have an effective cryptographic security parameter bitlength of minimal 125 bit; and
- derived tokens have a time during which a token is valid of maximal 10 minutes (600 seconds); and
- all derived tokens than can be valid at the same time have a combined probability of guessing a cryptographic parameter of maximal $10^{-5}$ within the time during which a token is valid.

NOTE 1: The $p_{GRP}$ allows for a tradeoff between complexity of passwords or PINs and restrictions on the number of attempts to enter a password or PIN.

NOTE 2: The calculation of $L_{CP,eff}$ is based on the recommendations in [[@NIST-SP-800].

### E.1.1.11 [AUM-E-MFA-Enhanced] AUTH.Enhanced MFA

Where multiple authentication factors are used to achieve AUTH.Enhanced, the authentication mechanism shall ensure that:

- at least two authentication factors are of different types (inherence, knowledge or possession); and
- it fulfils the respective SFA requirements of at least AUTH.Medium with at least these two authentication factors; and
- that the authentication request is only considered valid if at least these two authentication factors are validated within maximal 15 minutes (900 seconds) of each other.

### E.1.1.12 [AUM-E-I-Strong] AUTH.Strong inherence based SFA

Where an authentication factor of the type inherence is used to achieve AUTH.Strong, the authentication mechanisms shall ensure a false acceptance rate of maximal $10^{-5}$ and a false rejection rate of maximal $3 \times 10^{-2}$.

NOTE: The values used for false acceptance rate and false rejection rate are based on ETSI TS 103 732-2 [i.6].

### E.1.1.13 [AUM-E-P-Strong] AUTH.Strong possession based SFA

Where a security token is used as a possession type authentication factor to achieve AUTH.Strong, the authentication mechanisms shall ensure that:

- confidential cryptographic keys cannot be extracted from a security token; and
- confidential cryptographic keys in security tokens have an effective cryptographic security parameter bitlength of minimal 125 bit; and
- derived tokens have a time during which a token is valid of maximal five minutes (300 seconds); and
- all derived tokens than can be valid at the same time have a combined probability of guessing a cryptographic parameter of maximal $10^{-6}$ within the time during which a token is valid.

NOTE 1: The $p_{GRP}$ allows for a tradeoff between complexity of passwords or PINs and restrictions on the number of attempts to enter a password or PIN.

NOTE 2: The calculation of $L_{CP,eff}$ is based on the recommendations in [[@NIST-SP-800].

### E.1.1.14 [AUM-E-MFA-Strong] AUTH.Strong MFA

Where multiple authentication factors are used to achieve AUTH.Strong, the authentication mechanism shall ensure that:

- at least two authentication factors are of different types (inherence, knowledge or possession); and
- it fulfils the respective SFA requirements of at least AUTH.Enhanced with all of these authentication factors; and
- that the authentication request is only considered valid if all of these authentication factors are validated within maximal 10 minutes of each other.

### E.1.1.15 [AUM-E-Replay] AUTH.Medium, AUTH.Enhanced and AUTH.Strong replay protection

Where authentication mechanisms are accessible via interfaces with local communication, adjacent communication or public communication and provide AUTH.Medium, AUTH.Enhanced or AUTH.Strong, the authentication mechanisms shall protect against authentication of a third entity (attacker) by interception and retransmission of valid transmissions between the personal wearable and another entity.

#### E.1.1.16 [AUM-E-PitM] AUTH.Medium, AUTH.Enhanced and AUTH.Strong person in the middle protection

Where authentication mechanisms are accessible via interfaces with local communication, adjacent communication or public communication and provide AUTH.Medium, AUTH.Enhanced or AUTH.Strong, the authentication mechanisms shall protect against authentication of a third entity (attacker) by interception and alteration of data transmissions between the personal wearable and the entity that requests authentication.

## E.1.2 Assessment for [AUM-FH] authentication mechanism strength

### E.1.2.1 General

Specific assessments on authentication mechanisms for the AUTH strength level determined in clause 5.6.2.

### E.1.2.2 Assessment criteria for [AUM-E-I-Basic]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the personal wearable to fulfil [AUM-FH] clause 5.6.2 for authentication level AUTH.Basic using inherence authentication factors

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the authentication mechanism used by the personal wearable to achieve AUTH.Basic using inherence authentication factors:
  - documentation of the authentication factors that can be used

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Basic is created
- a test setup to access the documented authentication mechanism via a documented interface

**Assessment activities:**

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces
- determine the FAR value of the authentication mechanism
- determine the FRR value of the authentication mechanism

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the authentication mechanism used to achieve AUTH.Basic with inherence authentication factors has a FAR of maximal $10^{-4}$; and
- the authentication mechanism used to achieve AUTH.Basic with inherence authentication factors has a FRR of maximal $10^{-1}$; and

- there is no indication, that the authentication mechanism used to achieve AUTH.Basic with inherence authentication factors differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test

### E.1.2.3 Assessment criteria for [AUM-E-K-Basic]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the personal wearable to fulfil [AUM-FH] clause 5.6.2 for authentication level AUTH.Basic using knowledge authentication factors

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the authentication mechanism used by the personal wearable to achieve AUTH.Basic using knowledge authentication factors:
  - documentation of the authentication factors that can be used.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Basic is created;
- a test setup to access the documented authentication mechanism via a documented interface.

**Assessment activities:**

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- determine the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) value of the authentication mechanism;
- determine the maximum sustained validation attempt frequency ($f_{VA,max}$) value of the authentication mechanism;
- calculate the probability of guessing a cryptographic parameter ($p_{GRP}$) for a security insurance time (security insurance time) of one day $p_{GRP} = T_{SI} \times f_{VA,max} / C_{CP,min}$.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the authentication mechanism used to achieve AUTH.Basic with knowledge authentication factors have a $p_{GRP}$ of maximal $10^{-2}$$ for a $T_{SI}$ of one day; and
- there is no indication, that the authentication mechanism used to achieve AUTH.Basic with knowledge authentication factors differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test

### E.1.2.4 Assessment criteria for [AUM-E-I-Medium]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the personal wearable to fulfil [AUM-FH] clause 5.6.2 for authentication level AUTH.Medium using inherence authentication factors

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the authentication mechanism used by the personal wearable to achieve AUTH.Medium using inherence authentication factors:
  - documentation of the authentication factors that can be used.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Medium is created;
- a test setup to access the documented authentication mechanism via a documented interface;

**Assessment activities:**

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- determine the FAR value of the authentication mechanism;
- determine the FRR value of the authentication mechanism.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the authentication mechanism used to achieve AUTH.Medium with inherence authentication factors has a FAR of maximal $5 \times 10^{-5}$; and
- the authentication mechanism used to achieve AUTH.Medium with inherence authentication factors has a FRR of maximal $10^{-1}$; and
- there is no indication, that an authentication mechanisms used to achieve AUTH.Medium with inherence authentication factors differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test

### E.1.2.5 Assessment criteria for [AUM-E-K-Medium]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the personal wearable to fulfil [AUM-FH] clause 5.6.2 for authentication level AUTH.Medium using knowledge authentication factors;

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the authentication mechanism used by the personal wearable to achieve AUTH.Medium using knowledge authentication factors:
  - documentation of the authentication factors that can be used.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Medium is created;
- a test setup to access the documented authentication mechanism via a documented interface.

**Assessment activities:**

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- determine the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) value of the authentication mechanism;
- determine the maximum sustained validation attempt frequency ($f_{VA,max}$) value of the authentication mechanism;
- calculate the probability of guessing a cryptographic parameter ($p_{GRP}$) for a security insurance time ($T_{SI}$) of one month ( $2{,}6 \times 10^6$ seconds ) $p_{GRP} = T_{SI} \times f_{VA,max} / C_{CP,min}$.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the authentication mechanism used to achieve AUTH.Medium with knowledge authentication factors have a $p_{GRP}$ of maximal $10^{-3}$ for a $T_{SI}$ of one month; and
- there is no indication, that the authentication mechanism used to achieve AUTH.Medium with knowledge authentication factors differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test

## E.1.2.6 Assessment criteria for [AUM-E-P-Medium]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the personal wearable to fulfil [AUM-FH] clause 5.6.2 for authentication level AUTH.Medium using possession authentication factors based on Accounts or Services

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the authentication mechanism used by the personal wearable to achieve AUTH.Medium using possession authentication factors based on Accounts or Services:
  - documentation of Accounts or Services that can be used by the authentication mechanism;

- documentation of how a security tokens authenticity is validated by the authentication mechanism.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Medium is created;
- a suitable security token is known to the authentication mechanism;
- a test setup to access the documented authentication mechanism via a documented interface.

**Assessment activities:**

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- where derived tokens are used to validate the authenticity of a security token:
  - determine the time during which a token is valid ($T_{VA}$) of the authentication mechanism for these derived tokens;
  - determine the maximal number of derived tokens, that can be valid at the same time ($n_{dt,max}$);
  - determine the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) value of the authentication mechanism;
  - determine the maximum sustained validation attempt frequency ($f_{VA,max}$) value of the authentication mechanism;
  - calculate the combined probability of guessing a cryptographic parameter ($p_{GRP}$) for the derived tokens, that can be valid at the same time: $p_{GRP} = T_{VA} \times f_{VA,max} \times n_{dt,max} / C_{CP,min}$.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- derived tokens have a time during which a token is valid of maximal 15 minutes (900 seconds); and
- derived tokens have a combined probability of guessing a cryptographic parameter of maximal $10^{-3}$; and
- there is no indication, that the authentication mechanisms used to achieve AUTH.Medium with possession authentication factor differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test

## E.1.2.7 Assessment criteria for [AUM-E-MFA-Medium]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the personal wearable to fulfil [AUM-FH] clause 5.6.2 for authentication level AUTH.Medium using MFA

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the authentication mechanism used by the personal wearable to achieve AUTH.Medium using MFA:
  - documentation of the authentication factors that can be used.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Medium is created;
- a test setup to access the documented authentication mechanism via a documented interface.

**Assessment activities:**

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- verify whether authentication factors of the same type can be used for MFA;
- for authentication factors based on knowledge, verify whether the authentication mechanism would satisfy the assessment clause E.1.2.3 (or clause E.1.2.5. clause E.1.2.9);
- for authentication factors based on inherence, verify whether the authentication mechanism would satisfy the assessment clause E.1.2.2 (or clause E.1.2.4. clause E.1.2.8, clause E.1.2.12);
- for authentication factors based on possession, verify whether the authentication mechanism would satisfy the assessment clause E.1.2.6 (or clause E.1.2.10, clause E.1.2.13);
- determine the maximal time between entering the first and the last authentication factor for an authentication attempt to be successful.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- at least two authentication factors are of different types are necessary for a successful authentication; and
- satisfies the assessment for AUTH.Medium or higher with at least these two authentication factors; and
- at least these two authentication factors have to be validated within maximal 15 minutes (900 seconds) of each other for a successful authentication; and
- there is no indication, that the authentication mechanism used to achieve AUTH.Medium with MFA differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test

### E.1.2.8 Assessment criteria for [AUM-E-I-Enhanced]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the personal wearable to fulfil [AUM-FH] clause 5.6.2 for authentication level AUTH.Enhanced using inherence authentication factors;

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the authentication mechanism used by the personal wearable to achieve AUTH.Enhanced using inherence authentication factors:
  - documentation of the authentication factors that can be used

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Enhanced is created;
- a test setup to access the documented authentication mechanism via a documented interface.

**Assessment activities:**

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- determine the FAR value of the authentication mechanism;
- determine the FRR value of the authentication mechanism.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the authentication mechanism used to achieve AUTH.Enhanced with inherence authentication factors has a FAR of maximal $2 \times 10^{-5}$; and
- the authentication mechanism used to achieve AUTH.Enhanced with inherence authentication factors has a FRR of maximal $3 \times 10^{-2}$; and
- there is no indication, that the authentication mechanism used to achieve AUTH.Enhanced with inherence authentication factors differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test

### E.1.2.9 Assessment criteria for [AUM-E-K-Enhanced]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the personal wearable to fulfil [AUM-FH] clause 5.6.2 for authentication level AUTH.Enhanced using knowledge authentication factors;

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the authentication mechanism used by the personal wearable to achieve AUTH.Enhanced using knowledge authentication factors:
  - documentation of the authentication factors that can be used.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Enhanced is created;
- a test setup to access the documented authentication mechanism via a documented interface.

**Assessment activities:**

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- determine the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) value of the authentication mechanism;
- determine the maximum sustained validation attempt frequency ($f_{VA,max}$) value of the authentication mechanism;
- calculate the probability of guessing a cryptographic parameter ($p_{GRP}$) for a security insurance time ($T_{SI}$) of one year ($3.2 \times 10^7$ seconds ) $p_{GRP} = T_{SI} \times f_{VA,max} / C_{CP,min}$.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the authentication mechanism used to achieve AUTH.Enhanced with knowledge authentication factors have a $p_{GRP}$ of maximal $10^{-5}$ for a $T_{SI}$ of one year; and
- there is no indication, that the authentication mechanism used to achieve AUTH.Enhanced with knowledge authentication factors differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test

## E.1.2.10 Assessment criteria for [AUM-E-P-Enhanced]

Where an Account or Service is used as an authentication factor of the type possession for authentication level AUTH.Enhanced, the following assessment has to be performed: **Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the personal wearable to fulfil [AUM-FH] clause 5.6.2 for authentication level AUTH.Enhanced using possession authentication factors based on Accounts or Services;

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the authentication mechanism used by the personal wearable to achieve AUTH.Enhanced using possession authentication factors based on Accounts or Services:
  - documentation of Accounts or Services that can be used by the authentication mechanism;
  - documentation of how a security tokens authenticity is validated by the authentication mechanism.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Enhanced is created;
- a suitable security token is known to the authentication mechanism;

- a test setup to access the documented authentication mechanism via a documented interface.

**Assessment activities:**

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- where derived tokens are used to validate the authenticity of a security token:
  - determine the time during which a token is valid ($T_{VA}$) of the authentication mechanism for these derived tokens;
  - determine the maximal number of derived tokens, that can be valid at the same time ($n_{dt,max}$);
  - determine the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) value of the authentication mechanism;
  - determine the maximum sustained validation attempt frequency ($f_{VA,max}$) value of the authentication mechanism;
  - calculate the combined probability of guessing a cryptographic parameter ($p_{GRP}$) for the derived tokens, that can be valid at the same time: $p_{GRP} = T_{VA} \times f_{VA,max} \times n_{dt,max} / C_{CP,min}$.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- derived tokens have a time during which a token is valid of maximal 10 minutes; and
- derived tokens have a combined probability of guessing a cryptographic parameter of maximal $10^{-4}$; and
- there is no indication, that the authentication mechanism used to achieve AUTH.Enhanced with possession authentication factor differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test.

Where a security token is used as an authentication factor of the type possession for authentication level AUTH.Enhanced, the following assessment has to be performed: **Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the personal wearable to fulfil [AUM-FH] clause 5.6.2 for authentication level AUTH.Enhanced using possession authentication factors based on security tokens;

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the authentication mechanism used by the personal wearable to achieve AUTH.Enhanced using possession authentication factors based on security tokens:
  - documentation of security tokens that can be used by the authentication mechanism.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Enhanced is created;
- suitable security tokens for user with the documented authentication mechanisms;

- a test setup to access the documented authentication mechanism via a documented interface.

**Assessment activities:**

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- determine the minimal effective cryptographic security parameter bitlength of the security tokens that can be used by the authentication mechanism;
- where derived tokens are used to validate the authenticity of a security token:
  - determine the time during which a token is valid ($T_{VA}$) of the authentication mechanism for derived tokens;
  - determine the maximal number of derived tokens, that can be valid at the same time ($n_{dt,max}$);
  - determine the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) value of the derived tokens;
  - determine the maximum sustained validation attempt frequency ($f_{VA,max}$) value of the authentication mechanism;
  - calculate the combined probability of guessing a cryptographic parameter ($p_{GRP}$) for the derived tokens, that can be valid at the same time: $p_{GRP} = T_{VA} \times f_{VA,max} \times n_{dt,max} / C_{CP,min}$.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- security tokens have an effective cryptographic security parameter bitlength of minimal 125 bit; and
- derived tokens have a time during which a token is valid of maximal 10 minutes; and
- derived tokens have a combined probability of guessing a cryptographic parameter of maximal $10^{-5}$; and
- there is no indication, that the authentication mechanism used to achieve AUTH.Enhanced with possession authentication factor differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test

## E.1.2.11 Assessment criteria for [AUM-E-MFA-Enhanced]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the personal wearable to fulfil [AUM-FH] clause 5.6.2 for authentication level AUTH.Enhanced using MFA;

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the authentication mechanism used by the personal wearable to achieve AUTH.Enhanced using MFA:
  - documentation of the authentication factors that can be used.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Enhanced is created;
- a test setup to access the documented authentication mechanism via a documented interface.

**Assessment activities:**

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- verify whether authentication factors of the same type can be used for MFA;
- for authentication factors based on knowledge, verify whether the authentication mechanism would satisfy the assessment clause E.1.2.5 (or clause E.1.2.9);
- for authentication factors based on inherence, verify whether the authentication mechanism would satisfy the assessment clause E.1.2.4 (or clause E.1.2.8, clause E.1.2.12);
- for authentication factors based on possession, verify whether the authentication mechanism would satisfy the assessment clause E.1.2.6 (or clause E.1.2.10, clause E.1.2.13);
- determine the maximal time between entering the first and the last authentication factor for an authentication attempt to be successful.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- at least two authentication factors are of different types are necessary for a successful authentication; and
- satisfies the assessment for AUTH.Medium or higher with at least these two authentication factors; and
- at least these two authentication factors have to be validated within maximal 10 minutes (600 seconds) of each other for a successful authentication; and
- there is no indication, that the authentication mechanism used to achieve AUTH.Enhanced with MFA differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test.

## E.1.2.12 Assessment criteria for [AUM-E-I-Strong]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the personal wearable to fulfil [AUM-FH] clause 5.6.2 for authentication level AUTH.Strong using inherence authentication factors;

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the authentication mechanism used by the personal wearable to achieve AUTH.Strong using inherence authentication factors:
  - documentation of the authentication factors that can be used.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Strong is created;
- a test setup to access the documented authentication mechanism via a documented interface.

**Assessment activities:**

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- determine the FAR value of the authentication mechanism;
- determine the FRR value of the authentication mechanism.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the authentication mechanism used to achieve AUTH.Strong with inherence authentication factors has a FAR of maximal $10^{-5}$; and
- the authentication mechanism used to achieve AUTH.Strong with inherence authentication factors has a FRR of maximal $3 \times 10^{-2}$; and
- there is no indication, that the authentication mechanism used to achieve AUTH.Strong with inherence authentication factors differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test

## E.1.2.13 Assessment criteria for [AUM-E-P-Strong]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the personal wearable to fulfil [AUM-FH] clause 5.6.2 for authentication level AUTH.Strong using possession authentication factors based on security tokens;

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the authentication mechanism used by the personal wearable to achieve AUTH.Strong using possession authentication factors based on security tokens:
  - documentation of security tokens that can be used by the authentication mechanism.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Strong is created;
- suitable security tokens for user with the documented authentication mechanisms;
- a test setup to access the documented authentication mechanism via a documented interface.

**Assessment activities:**

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- determine the minimal effective cryptographic security parameter bitlength of the security tokens that can be used by the authentication mechanism;
- where derived tokens are used to validate the authenticity of a security token:
  - determine the time during which a token is valid ($T_{VA}$) of the authentication mechanism for derived tokens;
  - determine the maximal number of derived tokens, that can be valid at the same time ($n_{dt,max}$);
  - determine the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) value of the derived tokens;
  - determine the maximum sustained validation attempt frequency ($f_{VA,max}$) value of the authentication mechanism;
  - calculate the combined probability of guessing a cryptographic parameter ($p_{GRP}$) for the derived tokens, that can be valid at the same time: $p_{GRP} = T_{VA} \times f_{VA,max} \times n_{dt,max} / C_{CP,min}$.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- security tokens have an effective cryptographic security parameter bitlength of minimal 125 bit; and
- derived tokens have a time during which a token is valid of maximal five minutes; and
- derived tokens have a combined probability of guessing a cryptographic parameter of maximal $10^{-4}$; and
- there is no indication, that an authentication mechanisms used to achieve AUTH.Strong with possession authentication factor differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test

## E.1.2.14 Assessment criteria for [AUM-E-MFA-Strong]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the personal wearable to fulfil [AUM-FH] clause 5.6.2 for authentication level AUTH.Strong using MFA;

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the authentication mechanism used by the personal wearable to achieve AUTH.Strong using MFA:
  - documentation of the authentication factors that can be used.

The following test setups shall be prepared:

- a test user with permissions that necessitate authentication level AUTH.Strong is created;

- a test setup to access the documented authentication mechanism via a documented interface.

**Assessment activities:**

The following activities shall be performed:

- verify whether the authentication mechanism can be accessed via the documented interfaces;
- verify whether authentication factors of the same type can be used for MFA;
- for authentication factors based on knowledge, verify whether the authentication mechanism would satisfy the assessment clause E.1.2.9;
- for authentication factors based on inherence, verify whether the authentication mechanism would satisfy the assessment clause E.1.2.8 (or clause E.1.2.12);
- for authentication factors based on possession, verify whether the authentication mechanism would satisfy the assessment clause E.1.2.10 (or clause E.1.2.13);
- determine the maximal time between entering the first and the last authentication factor for an authentication attempt to be successful.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- at least two authentication factors are of different types are necessary for a successful authentication; and
- satisfies the assessment for AUTH.Medium or higher with all of these authentication factors; and
- all of these authentication factors have to be validated within 5 minutes (300 seconds) of each other for a successful authentication; and
- there is no indication, that the authentication mechanism used to achieve AUTH.Strong with MFA differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test

## E.1.2.15 Assessment criteria for [AUM-E-Replay]

**Assessment objective:**

The assessment covers:

- a functional assessment of authentication mechanisms that are accessible via interfaces with local communication, adjacent communication or public communication and provide AUTH.Medium, AUTH.Enhanced or AUTH.Strong.

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the authentication mechanism that are accessible via interfaces with local communication, adjacent communication or public communication and provide AUTH.Medium, AUTH.Enhanced or AUTH.Strong:
  - documentation of the communication protocols uses for the authentication process

The following test setups shall be prepared:

- a communication partner with active authentication mechanisms shall be set up for the personal wearable;

- a capture and replay tool between personal wearable and its communication partner shall be set up;
- at least one interface, where the authentication mechanism is reachable shall be documented.

**Assessment activities:**

The following activities shall be performed:

- authentication mechanisms that are accessible via interfaces with local communication, adjacent communication or public communication and provide AUTH.Medium, AUTH.Enhanced or AUTH.Strong:
  - Initiate a connection between the personal wearable and its communication partner.
  - Use a capture tool to record the transmitted message or transaction data.
  - Replay (retransmit) the captured message to the authentication mechanism using a suitable tool in place to mimic the original communication partner.
  - Record if the authentication mechanism accepts the retransmitted data

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the authentication mechanism does not accept the retransmitted data as valid authentication attempts.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

## E.1.2.16 Assessment criteria for [AUM-E-PitM]

**Assessment objective:**

The assessment covers:

- a functional assessment of authentication mechanisms that are accessible via interfaces with local communication, adjacent communication or public communication and provide AUTH.Medium, AUTH.Enhanced or AUTH.Strong;

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the authentication mechanism that are accessible via interfaces with local communication, adjacent communication or public communication and provide AUTH.Medium, AUTH.Enhanced or AUTH.Strong:
  - documentation of the communication protocols uses for the authentication process.

The following test setups shall be prepared:

- a communication partner with active authentication mechanisms shall be set up for the personal wearable;
- a capture and PitM tool between personal wearable and its communication partner shall be set up;
- at least one interface, where the authentication mechanism is reachable shall be documented;

**Assessment activities:**

The following activities shall be performed:

- authentication mechanisms that are accessible via interfaces with local communication, adjacent communication or public communication and provide AUTH.Medium, AUTH.Enhanced or AUTH.Strong:
  - Initiate a connection between the personal wearable and its communication partner.
  - Attempt to capture data (user credentials, tokens, etc.) with the tool in place and actively intercept communication to impersonate the communication partner during:
    - generation and communication of authentication factor for the communication partner (if not pre-configured); and
    - authentication of the communication partner:

      Record if the impersonation as communication partner is successful

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the authentication mechanism does not accept the PitM as an authenticated entity.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

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

# E.2 integrity protection strength

## E.2.1 [INT-SSM] Integrity protecting persistent storage for integrity relevant data

### E.2.1.1 General

Specific requirements on integrity protecting secure storage mechanisms for the INT-SSM strength level determined in clause 5.8.1.

### E.2.1.2 [INT-SSM-E-Basic] INT.SSM.Basic integrity protecting secure storage mechanism

Where an integrity protecting secure storage mechanism is used to achieve INT.SSM.Basic, the integrity protecting secure storage mechanism shall use cryptographic protection measures to protect against targeted modification of stored data, using a confidential cryptographic key with a $L_{CP,eff}$ of minimal 112 bit.

NOTE: Protection against targeted modification of stored data can amongst others be achieved by appropriate storage encryption.

### E.2.1.3 [INT-SSM-E-Medium] INT.SSM.Medium integrity protecting secure storage mechanism

Where an integrity protecting secure storage mechanism is used to achieve INT.SSM.Medium, the integrity protecting secure storage mechanism shall:

- use cryptographic protection measures to protect against targeted modification of stored data, using a confidential cryptographic key with a $L_{CP,eff}$ of minimal 112 bit; and
- only decrypt after an authorized user is authenticated.

NOTE: Protection against targeted modification of stored data can amongst others be achieved by appropriate storage encryption.

### E.2.1.4 [INT-SSM-E-Enhanced] INT.SSM.Enhanced integrity protecting secure storage mechanism

Where an integrity protecting secure storage mechanism is used to achieve INT.SSM.Enhanced, the integrity protecting secure storage mechanism shall:

use cryptographic protection measures to protect against targeted modification of stored data, using a confidential cryptographic key with a $L_{CP,eff}$ of minimal 125 bit and - only decrypt after an authorized user is authenticated and - the is protected against unauthorized access by hardware measures.

NOTE: Protection against targeted modification of stored data can amongst others be achieved by appropriate storage encryption.

### E.2.1.5 [INT-SSM-E-Strong] INT.SSM.Strong integrity protecting secure storage mechanism

Where an integrity protecting secure storage mechanism is used to achieve INT.SSM.Strong, the integrity protecting secure storage mechanism shall prevent the physical modification of data by hardware.

## E.2.2 Assessment for integrity protecting secure storage mechanism strength

### E.2.2.1 General

Specific assessments on integrity protecting secure storage mechanisms for the INT-SSM strength level determined in clause 5.8.1.

### E.2.2.2 Assessment criteria for [INT-SSM-E-Basic]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of an integrity protecting secure storage mechanism used by the personal wearable to fulfil [INT-SSM] clause 5.8.1 for authentication level INT.SSM.Basic.

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the integrity protecting secure storage mechanism used by the personal wearable to achieve INT.SSM.Basic

- documentation of the confidential cryptographic keys used to protect against targeted modification of stored data

The following test setups shall be prepared:

- a test setup to access the documented integrity protecting secure storage mechanism

**Assessment activities:**

The following activities shall be performed:

- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect against targeted modification of stored data

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the integrity protecting secure storage mechanism used to achieve INT.SSM.Basic uses only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit to protect against targeted modification of stored data; and
- there is no indication, that the integrity protecting secure storage mechanism used to achieve INT.SSM.Basic differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test

### E.2.2.3 Assessment criteria for [INT-SSM-E-Medium]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of an integrity protecting secure storage mechanism used by the personal wearable to fulfil [INT-SSM] clause 5.8.1 for authentication level INT.SSM.Basic.

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the integrity protecting secure storage mechanism used by the personal wearable to achieve INT.SSM.Basic:
  - documentation of the confidential cryptographic keys used to protect against targeted modification of stored data

The following test setups shall be prepared:

- a test setup to access the documented integrity protecting secure storage mechanism

**Assessment activities:**

The following activities shall be performed:

- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect against targeted modification of stored data;
- verify whether stored integrity relevant data is not targeted modifiable until an authorized user is authenticated.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the integrity protecting secure storage mechanism used to achieve INT.SSM.Basic uses only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit to protect against targeted modification of stored data; and
- stored integrity relevant data is not targeted modifiable until an authorized user is authenticated; and
- there is no indication, that the integrity protecting secure storage mechanism used to achieve INT.SSM.Basic differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test.

### E.2.2.4 Assessment criteria for [INT-SSM-E-Enhanced]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of an integrity protecting secure storage mechanism used by the personal wearable to fulfil [INT-SSM] clause 5.8.1 for authentication level INT.SSM.Enhanced.

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the integrity protecting secure storage mechanism used by the personal wearable to achieve INT.SSM.Enhanced:
  - documentation of the confidential cryptographic keys used to protect against targeted modification of stored data

The following test setups shall be prepared:

- a test setup to access the documented integrity protecting secure storage mechanism

**Assessment activities:**

The following activities shall be performed:

- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect against targeted modification of stored data;
- verify whether stored integrity relevant data is not targeted modifiable until an authorized user is authenticated;
- verify whether confidential cryptographic keys used to protect against targeted modification of stored data is protected against unauthorized access by hardware measures.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the integrity protecting secure storage mechanism used to achieve INT.SSM.Enhanced uses only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 125 bit to protect against targeted modification of stored data; and

- stored integrity relevant data is not targeted modifiable until an authorized user is authenticated; and
- the confidential cryptographic keys used to protect against targeted modification of stored data is protected against unauthorized access by hardware measures; and
- there is no indication, that the integrity protecting secure storage mechanism used to achieve INT.SSM.Enhanced differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test.

### E.2.2.5 Assessment criteria for [INT-SSM-E-Strong]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of an integrity protecting secure storage mechanism used by the personal wearable to fulfil [INT-SSM] clause 5.8.1 for authentication level INT.SSM.Strong.

based on the default configuration required by clause 5.4.1

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the integrity protecting secure storage mechanism used by the personal wearable to achieve INT.SSM.Strong:
  - documentation of the hardware measures used to protect against targeted modification of stored data.

The following test setups shall be prepared:

- a test setup to access the documented integrity protecting secure storage mechanism.

**Assessment activities:**

The following activities shall be performed:

- verify whether against targeted modification of stored integrity relevant data is protected by hardware measures.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- against targeted modification of stored integrity relevant data is protected by hardware measures; and
- there is no indication, that the integrity protecting secure storage mechanism used to achieve INT.SSM.Strong differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test

## E.2.3 [INT-COM] Communication of integrity relevant data

### E.2.3.1 General

Specific requirements on integrity protecting communication mechanisms for the INT-COM strength level determined in clause 5.8.3. Note that for CONF.COM.Medium, CONF.COM.Enhanced and CONF.COM.Strong, the requirements in clause E.2.3.5 and clause E.2.3.6 are also to be considered.

### E.2.3.2 [INT-COM-E-Basic] INT.COM.Basic integrity protecting communication mechanism

Where an integrity protecting communication mechanism is used to achieve INT.COM.Basic, the integrity protecting communication mechanism shall use confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit to protect the integrity of communicated integrity relevant data.

NOTE: The values used for effective cryptographic security parameter bitlength are based on IETF RFC 8446 [i.8], IETF RFC 8613 [i.9], IETF RFC 9528 [i.10] and IETF RFC 9147 [i.11].

### E.2.3.3 [INT-COM-E-Medium] INT.COM.Medium integrity protecting communication mechanism

Where an integrity protecting communication mechanism is used to achieve INT.COM.Basic, the integrity protecting communication mechanism shall use confidential cryptographic keys with:

- a $L_{CP,eff}$ of minimal 112 bit; or
- where maximal 1GB of data of data can be communicated between rekeys due to bandwidth or power constraints, a $L_{CP,eff}$ of minimal 112 bit

to protect the integrity of communicated integrity relevant data.

NOTE: The values used for effective cryptographic security parameter bitlength are based on IETF RFC 8446 [i.8], IETF RFC 8613 [i.9], IETF RFC 9528 [i.10] and IETF RFC 9147 [i.11].

### E.2.3.4 [INT-COM-E-Enhanced] INT.COM.Enhanced integrity protecting communication mechanism

Where an integrity protecting communication mechanism is used to achieve INT.COM.Basic, the integrity protecting communication mechanism shall use confidential cryptographic keys with:

- a $L_{CP,eff}$ of minimal 125 bit; or
- where maximal 1GB of data of data can be communicated between rekeys due to bandwidth or power constraints, a $L_{CP,eff}$ of minimal 112 bit;

to protect the integrity of communicated integrity relevant data.

NOTE: The values used for effective cryptographic security parameter bitlength are based on IETF RFC 8446 [i.8], IETF RFC 8613 [i.9], IETF RFC 9528 [i.10] and IETF RFC 9147 [i.11].

### E.2.3.5 [INT-COM-E-EndAuth] INT.COM.Medium and INT.COM.Enhanced integrity protecting communication mechanism endpoint authentification

Where an integrity protecting communication mechanism is used to achieve INT.COM.Medium or INT.COM.Enhanced, the integrity protecting communication mechanism shall support the authentication of communication endpoints.

#### E.2.3.6 [INT-COM-E-Downgrade] INT.COM.Medium and INT.COM.Enhanced integrity protecting communication mechanism downgrade protection

Where an integrity protecting communication mechanism is used to achieve INT.COM.Medium or INT.COM.Enhanced, the integrity protecting communication mechanism shall support measures to prevent downgrade of the integrity protecting communication mechanisms protection measures below the protection strength level required in clause 5.8.3.

### E.2.4 Assessment for integrity protecting communication mechanism strength

#### E.2.4.1 General

Specific assessments on integrity protecting communication mechanisms for the INT-COM strength level determined in clause 5.8.3.

#### E.2.4.2 Assessment criteria for [INT-COM-E-Basic]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of an integrity protecting communication mechanism used by the personal wearable to fulfil [INT-COM] clause 5.8.3 for authentication level INT.COM.Basic;

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the integrity protecting communication mechanism used by the personal wearable to achieve INT.COM.Basic:
  - documentation of the confidential cryptographic keys used to protect the integrity of communicated integrity relevant data.

The following test setups shall be prepared:

- a test setup to access the documented integrity protecting communication mechanism via a documented interface.

**Assessment activities:**

The following activities shall be performed:

- verify whether the integrity protecting communication mechanism can be accessed via the documented interfaces;
- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect the integrity of communicated integrity relevant data.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the integrity protecting communication mechanism used to achieve INT.COM.Basic uses only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit to protect the integrity of communicated integrity relevant data; and

- there is no indication, that the integrity protecting communication mechanism used to achieve INT.COM.Basic differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test.

### E.2.4.3 Assessment criteria for [INT-COM-E-Medium]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of an integrity protecting communication mechanism used by the personal wearable to fulfil [INT-COM] clause 5.8.3 for authentication level INT.COM.Medium;

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the integrity protecting communication mechanism used by the personal wearable to achieve INT.COM.Medium:
  - documentation of the confidential cryptographic keys used to protect the integrity of communicated integrity relevant data;
  - where the integrity protecting communication mechanism is constrained by power or bandwidth:
    - the amount of data that can be communicated in a given time.

The following test setups shall be prepared:

- a test setup to access the documented integrity protecting communication mechanism via a documented interface.

**Assessment activities:**

The following activities shall be performed:

- verify whether the integrity protecting communication mechanism can be accessed via the documented interfaces;
- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect the integrity of communicated integrity relevant data:
  - if the $L_{CP,eff}$ is between 100 bit and 112 bit:
    - determine the time after which the confidential cryptographic keys used to protect the integrity of communicated integrity relevant data are renewed;
    - determine the amount of data that can be communicated during this time.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the integrity protecting communication mechanism used to achieve INT.COM.Medium uses only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit to protect the integrity of communicated integrity relevant data; or

- if amount of data can be communicated during the time between the renewal of confidential cryptographic keys used to protect the integrity of communicated integrity relevant data is maximal 1GB of data, only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit; and
- there is no indication, that the integrity protecting communication mechanism used to achieve INT.COM.Medium differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test.

### E.2.4.4 Assessment criteria for [INT-COM-E-Enhanced]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of an integrity protecting communication mechanism used by the personal wearable to fulfil [INT-COM] clause 5.8.3 for authentication level INT.COM.Enhanced.

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the integrity protecting communication mechanism used by the personal wearable to achieve INT.COM.Enhanced:
  - documentation of the confidential cryptographic keys used to protect the integrity of communicated integrity relevant data;
  - where the integrity protecting communication mechanism is constrained by power or bandwidth:
    - the amount of data that can be communicated in a given time.

The following test setups shall be prepared:

- a test setup to access the documented integrity protecting communication mechanism via a documented interface.

**Assessment activities:**

The following activities shall be performed:

- verify whether the integrity protecting communication mechanism can be accessed via the documented interfaces;
- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect the integrity of communicated integrity relevant data:
  - if the $L_{CP,eff}$ is between 112 bit and 125 bit:
    - determine the time after which the confidential cryptographic keys used to protect the integrity of communicated integrity relevant data are renewed;
    - determine the amount of data that can be communicated during this time.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the integrity protecting communication mechanism used to achieve INT.COM.Enhanced uses only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 125 bit to protect the integrity of communicated integrity relevant data; or
- if amount of data can be communicated during the time between the renewal of confidential cryptographic keys used to protect the integrity of communicated integrity relevant data is maximal 1GB of data, only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit; and
- there is no indication, that the integrity protecting communication mechanism used to achieve INT.COM.Enhanced differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test.

### E.2.4.5 Assessment criteria for [INT-COM-E-EndAuth]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of an integrity protecting communication mechanism used by the personal wearable to fulfil [INT-COM] clause 5.8.3 for authentication level INT.COM.Medium or INT.COM.Enhanced;

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the integrity protecting communication mechanism used by the personal wearable to achieve INT.COM.Medium or INT.COM.Enhanced:
  - documentation of the measures to verify the authenticity of communication endpoints and to authenticate the integrity protecting communication mechanism or the architectural component.

The following test setups shall be prepared:

- a test setup to access the documented integrity protecting communication mechanism via a documented interface.

**Assessment activities:**

The following activities shall be performed:

- verify whether the integrity protecting communication mechanism supports authentication of communication endpoints before sending integrity relevant data;
- verify whether the integrity protecting communication mechanism supports authentication of itself or its architectural component to communication endpoints before the communication of integrity relevant data.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the integrity protecting communication mechanism supports authentication of communication endpoints before sending integrity relevant data; and

- the integrity protecting communication mechanism supports authentication of itself or its architectural component to communication endpoints before the communication of integrity relevant data.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test

### E.2.4.6 Assessment criteria for [INT-COM-E-Downgrade]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of an integrity protecting communication mechanism used by the personal wearable to fulfil [INT-COM] clause 5.8.3 for authentication level INT.COM.Medium or INT.COM.Enhanced.

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the integrity protecting communication mechanism used by the personal wearable to achieve INT.COM.Medium or INT.COM.Enhanced:
  - documentation of the measures to prevent the downgrade of the integrity protecting communication mechanisms protection level by communication endpoints.

The following test setups shall be prepared:

- a test setup to access the documented integrity protecting communication mechanism via a documented interface;
- a test setup to alter parameters of communication protocols, determining e.g. used protocol versions or cipher suites.

**Assessment activities:**

The following activities shall be performed:

- verify whether the integrity protecting communication mechanism refuses to send integrity relevant data using communication protocol parameters that would result in a protection level below INT.COM.Medium or INT.COM.Enhanced respectively;
- verify whether the integrity protecting communication mechanism refuses alteration of communication protocol parameters that would result in a protection level below INT.COM.Medium or INT.COM.Enhanced during the communication of integrity relevant data.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the integrity protecting communication mechanism refuses to send integrity relevant data using communication protocol parameters that would result in a protection level below INT.COM.Medium or INT.COM.Enhanced respectively; and
- the integrity protecting communication mechanism refuses alteration of communication protocol parameters that would result in a protection level below INT.COM.Medium or INT.COM.Enhanced during the communication of integrity relevant data.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test

## E.2.5 [INT-SWPCK] Software package verification

### E.2.5.1 General

Specific requirements on software package verification mechanisms' strength for the INT-SWPCK strength level determined in clause 5.8.2.

### E.2.5.2 [INT-SWPCK-E-Basic] INT.SW.VER.Basic software package verification mechanism

Where a software package verification mechanism is used to achieve INT.SW.VER.Basic, the software package verification mechanism shall:

- explicitly obtain the confirmation of an authorized entity that the integrity and authenticity of a software package has been verified by the entity, where the software package's source is determined by the entity; or
- explicitly obtain the confirmation of an authorized entity that the authenticity of a software package has been verified by the entity and use a hash or checksum provided by the entity for the software package to verify its integrity, where the software package's source is determined by the entity.

### E.2.5.3 [INT-SWPCK-E-Medium] INT.SW.VER.Medium software package verification mechanism

Where a software package verification mechanism is used to achieve INT.SW.VER.Medium, the software package verification mechanism shall ensure that a software package has been obtained from a trusted source over a secure communication channel that meets INT.COM.Enhanced.

### E.2.5.4 [INT-SWPCK-E-Enhanced] INT.SW.VER.Enhanced software package verification mechanism

Where a software package verification mechanism is used to achieve INT.SW.VER.Enhanced, the software package verification mechanism shall verify the authenticity and integrity of a software package using cryptographic digital signature with a $L_{CP,eff}$ of minimal 125 bit.

## E.2.6 Assessment for integrity protecting communication mechanism strength

### E.2.6.1 General

Specific assessments on integrity protecting communication mechanisms for the INT-SWPCK strength level determined in clause 5.8.2.

### E.2.6.2 Assessment criteria for [INT-SWPCK-E-Basic]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of a software package verification mechanism used by the personal wearable to fulfil [INT-SWPCK] clause 5.8.2 for authentication level INT.SW.VER.Basic.

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the software package verification mechanism used by the personal wearable to achieve INT.SW.VER.Basic:
  - documentation of the measures to confirm, that the and of a software package has been verified

The following test setups shall be prepared:

- a test identity with permissions to perform a software update using the software package verification mechanism;
- a software package to perform a software update;
- a test setup to access the documented software package verification mechanism and perform a software update.

**Assessment activities:**

The following activities shall be performed:

- verify whether the confirmation of an authorized identity that the and of a software package has been verified by the authorized identity is explicitly obtained by the software package verification mechanism used to achieve INT.SW.VER.Basic; or
- verify whether the confirmation of an authorized identity that the of a software package has been verified by the authorized identity is explicitly obtained by the software package verification mechanism used to achieve INT.SW.VER.Basic; and
  - verify whether an authorized identity is provided with a hash or checksum to verify the of a software package by the software package verification mechanism used to achieve INT.SW.VER.Basic

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the confirmation of an authorized identity that the and of a software package has been verified by the authorized identity is explicitly obtained by the software package verification mechanism used to achieve INT.SW.VER.Basic; or
- the confirmation of an authorized identity that the of a software package has been verified by the authorized identity is explicitly obtained by the software package verification mechanism used to achieve INT.SW.VER.Basic; and
  - an authorized identity is provided with a hash or checksum to verify the of a software package by the software package verification mechanism used to achieve INT.SW.VER.Basic; and
- there is no indication, that by the software package verification mechanism used to achieve INT.SW.VER.Basic differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test.

### E.2.6.3 Assessment criteria for [INT-SWPCK-E-Medium]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of a software package verification mechanism used by the personal wearable to fulfil [INT-SWPCK] clause 5.8.2 for authentication level INT.SW.VER.Medium.

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the software package verification mechanism used by the personal wearable to achieve INT.SW.VER.Medium:
  - documentation of the measures to ensure that a software package has been obtained from a trusted source over a secure communication channel:
    - list of trusted source of software packages; or
    - documentation on criteria what comprises a trusted source of software packages.

The following test setups shall be prepared:

- a test identity with permissions to perform a software update using the software package verification mechanism;
- a communication connection to a trusted source of software packages to perform a software update;
- a test setup to access the documented software package verification mechanism and perform a software update.

**Assessment activities:**

The following activities shall be performed:

- verify whether the software package verification mechanism ensures that a software package has been obtained from a trusted source over a secure communication channel;
- verify whether the secure communication channel over which the software package has been obtained fulfils clause E.2.3.4, clause E.2.3.5 and clause E.2.3.6.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the software package verification mechanism ensures that a software package has been obtained from a trusted source over a secure communication channel; and
- the secure communication channel over which the software package has been obtained fulfils clause E.2.3.4, clause E.2.3.5 and clause E.2.3.6; and
- there is no indication, that by the software package verification mechanism used to achieve INT.SW.VER.Medium differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test.

### E.2.6.4 Assessment criteria for [INT-SWPCK-E-Enhanced]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of a software package verification mechanism used by the personal wearable to fulfil [INT-SWPCK] clause 5.8.2 for authentication level INT.SW.VER.Enhanced.

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the software package verification mechanism used by the personal wearable to achieve INT.SW.VER.Enhanced:
  - documentation of the measures to verify the and of a software package using cryptographic digital signatures:
    - documentation of the cryptographic digital signatures used to verify the and of a software package.

The following test setups shall be prepared:

- a test identity with permissions to perform a software update using the software package verification mechanism;
- software packages to perform a software update;
- a test setup to access the documented software package verification mechanism and perform a software update.

**Assessment activities:**

The following activities shall be performed:

- verify whether the software package verification mechanism verifies the and of a software package using cryptographic digital signatures;
- determine the $L_{CP,eff}$ of the cryptographic digital signatures used to verify the and of a software package.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the software package verification mechanism verifies the and of a software package using cryptographic digital signatures; and
- the cryptographic digital signatures used to verify the and of a software package have a $L_{CP,eff}$ of minimal 125 bit; and
- there is no indication, that by the software package verification mechanism used to achieve INT.SW.VER.Enhanced differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test.

# E.3 confidentiality protection strength

## E.3.1 [CONF-SSM] Confidentiality protecting persistent storage for confidential data

### E.3.1.1 General

Specific requirements on integrity protecting secure storage mechanisms for the CONF-SSM strength level determined in clause 5.7.1.

#### E.3.1.2 [CONF-SSM-E-Basic] CONF.SSM.Basic confidentiality protecting secure storage mechanism

Where a confidentiality protecting secure storage mechanism is used to achieve CONF.SSM.Basic, the confidentiality protecting secure storage mechanism shall use cryptographic protection measures to protect the confidentiality of its stored confidential data, using a confidential cryptographic key with a $L_{CP,eff}$ of minimal 112 bit.

NOTE: The values used for effective cryptographic security parameter bitlength are based on IETF RFC 8446 [i.8], IETF RFC 8613 [i.9], IETF RFC 9528 [i.10] and IETF RFC 9147 [i.11].

#### E.3.1.3 [CONF-SSM-E-Medium] CONF.SSM.Medium confidentiality protecting secure storage mechanism

Where a confidentiality protecting secure storage mechanism is used to achieve CONF.SSM.Medium, the confidentiality protecting secure storage mechanism shall:

- use cryptographic protection measures to protect the confidentiality of its stored confidential data, using a confidential cryptographic key with a $L_{CP,eff}$ of minimal 112 bit; and
- only decrypt after an authorized user is authenticated.

NOTE: The values used for effective cryptographic security parameter bitlength are based on IETF RFC 8446 [i.8], IETF RFC 8613 [i.9], IETF RFC 9528 [i.10] and IETF RFC 9147 [i.11].

#### E.3.1.4 [CONF-SSM-E-Enhanced] CONF.SSM.Enhanced confidentiality protecting secure storage mechanism

Where a confidentiality protecting secure storage mechanism is used to achieve CONF.SSM.Enhanced, the confidentiality protecting secure storage mechanism shall:

- use cryptographic protection measures to protect the confidentiality of its stored confidential data, using a confidential cryptographic key with a $L_{CP,eff}$ of minimal 125 bit and - only decrypt after an authorized user is authenticated and - the is protected against unauthorized access by hardware measures.

NOTE: The values used for effective cryptographic security parameter bitlength are based on IETF RFC 8446 [i.8], IETF RFC 8613 [i.9], IETF RFC 9528 [i.10] and IETF RFC 9147 [i.11].

#### E.3.1.5 [CONF-SSM-E-Strong] CONF.SSM.Strong confidentiality protecting secure storage mechanism

Where a confidentiality protecting secure storage mechanism is used to achieve CONF.SSM.Strong, the confidentiality protecting secure storage mechanism shall prevent extraction of its stored confidential data by hardware measures.

### E.3.2 Assessment for confidentiality protecting secure storage mechanism strength

#### E.3.2.1 General

Specific assessments on integrity protecting secure storage mechanisms for the CONF-SSM strength level determined in clause 5.7.1.

### E.3.2.2 Assessment criteria for [CONF-SSM-E-Basic]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of a confidentiality protecting secure storage mechanism used by the personal wearable to fulfil [CONF-SSM] clause 5.7.1 for authentication level CONF.SSM.Medium.

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the confidentiality protecting secure storage mechanism used by the personal wearable to achieve CONF.SSM.Medium:
  - documentation of the confidential cryptographic keys used to protect the confidentiality of stored confidential data.

The following test setups shall be prepared:

- a test setup to access the documented confidentiality protecting secure storage mechanism.

**Assessment activities:**

The following activities shall be performed:

- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect the confidentiality of stored confidential data.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the confidentiality protecting secure storage mechanism used to achieve CONF.SSM.Medium uses only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit to protect the confidentiality of stored confidential data; and
- there is no indication, that the confidentiality protecting secure storage mechanism used to achieve CONF.SSM.Medium differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test.

### E.3.2.3 Assessment criteria for [CONF-SSM-E-Medium]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of a confidentiality protecting secure storage mechanism used by the personal wearable to fulfil [CONF-SSM] clause 5.7.1 for authentication level CONF.SSM.Basic.

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the confidentiality protecting secure storage mechanism used by the personal wearable to achieve CONF.SSM.Basic:
  - documentation of the confidential cryptographic keys used to protect the confidentiality of stored confidential data.

The following test setups shall be prepared:

- a test setup to access the documented confidentiality protecting secure storage mechanism.

**Assessment activities:**

The following activities shall be performed:

- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect the confidentiality of stored confidential data;
- verify whether stored confidential data is not readably in plain text until an authorized user is authenticated.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the confidentiality protecting secure storage mechanism used to achieve CONF.SSM.Basic uses only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit to protect the confidentiality of stored confidential data; and
- stored confidential data is not readably in plain text until an authorized user is authenticated; and
- there is no indication, that the confidentiality protecting secure storage mechanism used to achieve CONF.SSM.Basic differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test.

### E.3.2.4 Assessment criteria for [CONF-SSM-E-Enhanced]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of a confidentiality protecting secure storage mechanism used by the personal wearable to fulfil [CONF-SSM] clause 5.7.1 for authentication level CONF.SSM.Enhanced

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the confidentiality protecting secure storage mechanism used by the personal wearable to achieve CONF.SSM.Enhanced:
  - documentation of the confidential cryptographic keys used to protect the confidentiality of stored confidential data.

The following test setups shall be prepared:

- a test setup to access the documented confidentiality protecting secure storage mechanism.

**Assessment activities:**

The following activities shall be performed:

- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect the confidentiality of stored confidential data;
- verify whether stored confidential data is not readably in plain text until an authorized user is authenticated;
- verify whether confidential cryptographic keys used to protect the confidentiality of stored confidential data is protected against unauthorized access by hardware measures.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the confidentiality protecting secure storage mechanism used to achieve CONF.SSM.Enhanced uses only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 125 bit to protect the confidentiality of stored confidential data; and
- stored confidential data is not readably in plain text until an authorized user is authenticated; and
- the confidential cryptographic keys used to protect the confidentiality of stored confidential data is protected against unauthorized access by hardware measures; and
- there is no indication, that the confidentiality protecting secure storage mechanism used to achieve CONF.SSM.Enhanced differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test.

### E.3.2.5 Assessment criteria for [CONF-SSM-E-Strong]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of a confidentiality protecting secure storage mechanism used by the personal wearable to fulfil [CONF-SSM] clause 5.7.1 for authentication level CONF.SSM.Strong;

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the confidentiality protecting secure storage mechanism used by the personal wearable to achieve CONF.SSM.Strong:
  - documentation of the hardware measures used to protect the confidentiality of stored confidential data.

The following test setups shall be prepared:

- a test setup to access the documented confidentiality protecting secure storage mechanism.

**Assessment activities:**

The following activities shall be performed:

- verify whether the confidentiality of stored confidential data is protected by hardware measures.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the confidentiality of stored confidential data is protected by hardware measures; and
- there is no indication, that the confidentiality protecting secure storage mechanism used to achieve CONF.SSM.Strong differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test.

## E.3.3 [CONF-COM] Communication of confidential data

### E.3.3.1 General

Specific requirements on confidentiality protecting communication mechanisms for the CONF-COM strength level determined in clause 5.7.2. Note that for CONF.COM.Medium, CONF.COM.Enhanced and CONF.COM.Strong, the requirements in clause E.3.3.5 and clause E.3.3.6 are also to be considered.

### E.3.3.2 [CONF-COM-E-Basic] CONF.COM.Basic confidentiality protecting communication mechanism

Where a confidentiality protecting communication mechanism is used to achieve CONF.COM.Basic, the confidentiality protecting communication mechanism shall use confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit to protect the confidentiality of communicated confidential data.

NOTE: The values used for effective cryptographic security parameter bitlength are based on IETF RFC 8446 [i.8], IETF RFC 8613 [i.9], IETF RFC 9528 [i.10] and IETF RFC 9147 [i.11].

### E.3.3.3 [CONF-COM-E-Medium] CONF.COM.Medium confidentiality protecting communication mechanism

Where a confidentiality protecting communication mechanism is used to achieve CONF.COM.Basic, the confidentiality protecting communication mechanism shall use confidential cryptographic keys with:

- a $L_{CP,eff}$ of minimal 112 bit; or
- where maximal 1 GB of data of data can be communicated between rekeys due to bandwidth or power constraints, a $L_{CP,eff}$ of minimal 112 bit;

to protect the confidentiality of communicated confidential data.

NOTE: The values used for effective cryptographic security parameter bitlength are based on IETF RFC 8446 [i.8], IETF RFC 8613 [i.9], IETF RFC 9528 [i.10] and IETF RFC 9147 [i.11].

### E.3.3.4 [CONF-COM-E-Enhanced] CONF.COM.Enhanced confidentiality protecting communication mechanism

Where a confidentiality protecting communication mechanism is used to achieve CONF.COM.Basic, the confidentiality protecting communication mechanism shall use confidential cryptographic keys with:

- a $L_{CP,eff}$ of minimal 125 bit; or
- where maximal 1 GB of data of data can be communicated between rekeys due to bandwidth or power constraints, a $L_{CP,eff}$ of minimal 112 bit;

to protect the confidentiality of communicated confidential data.

NOTE: The values used for effective cryptographic security parameter bitlength are based on IETF RFC 8446 [i.8], IETF RFC 8613 [i.9], IETF RFC 9528 [i.10] and IETF RFC 9147 [i.11].

#### E.3.3.5 [CONF-COM-E-EndAuth] CONF.COM.Medium and CONF.COM.Enhanced confidentiality protecting communication mechanism endpoint authentification

Where a confidentiality protecting communication mechanism is used to achieve CONF.COM.Medium or CONF.COM.Enhanced, the confidentiality protecting communication mechanism shall support the authentication of communication endpoints.

#### E.3.3.6 [CONF-COM-E-Downgrade] CONF.COM.Medium and CONF.COM.Enhanced confidentiality protecting communication mechanism downgrade protection

Where a confidentiality protecting communication mechanism is used to achieve CONF.COM.Medium or CONF.COM.Enhanced, the confidentiality protecting communication mechanism shall support measures to prevent downgrade of the confidentiality protecting communication mechanisms protection measures below the protection strength level required in clause 5.7.2.

### E.3.4 Assessment for confidentiality protecting communication mechanism strength

#### E.3.4.1 General

Specific assessments on confidentiality protecting communication mechanisms for the CONF-COM strength level determined in clause 5.7.2.

#### E.3.4.2 Assessment criteria for [CONF-COM-E-Basic]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of a confidentiality protecting communication mechanism used by the personal wearable to fulfil [CONF-COM] clause 5.7.2 for authentication level CONF.COM.Basic.

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the confidentiality protecting communication mechanism used by the personal wearable to achieve CONF.COM.Basic:
  - documentation of the confidential cryptographic keys used to protect the confidentiality of communicated confidential data.

The following test setups shall be prepared:

- a test setup to access the documented confidentiality protecting communication mechanism via a documented interface.

**Assessment activities:**

The following activities shall be performed:

- verify whether the confidentiality protecting communication mechanism can be accessed via the documented interfaces;
- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect the confidentiality of communicated confidential data.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the confidentiality protecting communication mechanism used to achieve CONF.COM.Basic uses only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit to protect the confidentiality of communicated confidential data; and
- there is no indication, that the confidentiality protecting communication mechanism used to achieve CONF.COM.Basic differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test.

### E.3.4.3 Assessment criteria for [CONF-COM-E-Medium]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of a confidentiality protecting communication mechanism used by the personal wearable to fulfil [CONF-COM] clause 5.7.2 for authentication level CONF.COM.Medium.

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the confidentiality protecting communication mechanism used by the personal wearable to achieve CONF.COM.Medium:
  - documentation of the confidential cryptographic keys used to protect the confidentiality of communicated confidential data;
  - where the confidentiality protecting communication mechanism is constrained by power or bandwidth:
    - the amount of data that can be communicated in a given time.

The following test setups shall be prepared:

- a test setup to access the documented confidentiality protecting communication mechanism via a documented interface.

**Assessment activities:**

The following activities shall be performed:

- verify whether the confidentiality protecting communication mechanism can be accessed via the documented interfaces;

- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect the confidentiality of communicated confidential data:
  - if the $L_{CP,eff}$ is between 100 bit and 112 bit:
    - determine the time after which the confidential cryptographic keys used to protect the confidentiality of communicated confidential data are renewed;
    - determine the amount of data that can be communicated during this time.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the confidentiality protecting communication mechanism used to achieve CONF.COM.Medium uses only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit to protect the confidentiality of communicated confidential data; or
- if amount of data can be communicated during the time between the renewal of confidential cryptographic keys used to protect the confidentiality of communicated confidential data is maximal 1GB of data, only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit; and
- there is no indication, that the confidentiality protecting communication mechanism used to achieve CONF.COM.Medium differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test.

### E.3.4.4 Assessment criteria for [CONF-COM-E-Enhanced]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of a confidentiality protecting communication mechanism used by the personal wearable to fulfil [CONF-COM] clause 5.7.2 for authentication level CONF.COM.Enhanced;

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the confidentiality protecting communication mechanism used by the personal wearable to achieve CONF.COM.Enhanced:
  - documentation of the confidential cryptographic keys used to protect the confidentiality of communicated confidential data;
  - where the confidentiality protecting communication mechanism is constrained by power or bandwidth:
    - the amount of data that can be communicated in a given time.

The following test setups shall be prepared:

- a test setup to access the documented confidentiality protecting communication mechanism via a documented interface.

**Assessment activities:**

The following activities shall be performed:

- verify whether the confidentiality protecting communication mechanism can be accessed via the documented interfaces;
- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect the confidentiality of communicated confidential data:
  - if the $L_{CP,eff}$ is between 112 bit and 125 bit:
    - determine the time after which the confidential cryptographic keys used to protect the confidentiality of communicated confidential data are renewed;
    - determine the amount of data that can be communicated during this time.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the confidentiality protecting communication mechanism used to achieve CONF.COM.Enhanced uses only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 125 bit to protect the confidentiality of communicated confidential data; or
- if amount of data can be communicated during the time between the renewal of confidential cryptographic keys used to protect the confidentiality of communicated confidential data is maximal 1GB of data, only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit; and
- there is no indication, that the confidentiality protecting communication mechanism used to achieve CONF.COM.Enhanced differs from the documentation.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test.

### E.3.4.5 Assessment criteria for [CONF-COM-E-EndAuth]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of a confidentiality protecting communication mechanism used by the personal wearable to fulfil [CONF-COM] clause 5.7.2 for authentication level CONF.COM.Medium or CONF.COM.Enhanced;

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the confidentiality protecting communication mechanism used by the personal wearable to achieve CONF.COM.Medium or CONF.COM.Enhanced:
  - documentation of the measures to verify the authenticity of communication endpoints and to authenticate the confidentiality protecting communication mechanism or the architectural component.

The following test setups shall be prepared:

- a test setup to access the documented confidentiality protecting communication mechanism via a documented interface.

**Assessment activities:**

The following activities shall be performed:

- verify whether the confidentiality protecting communication mechanism supports authentication of communication endpoints before sending confidential data;
- verify whether the confidentiality protecting communication mechanism supports authentication of itself or its architectural component to communication endpoints before the communication of confidential data.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the confidentiality protecting communication mechanism supports authentication of communication endpoints before sending confidential data; and
- the confidentiality protecting communication mechanism supports authentication of itself or its architectural component to communication endpoints before the communication of confidential data.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test.

### E.3.4.6 Assessment criteria for [CONF-COM-E-Downgrade]

**Assessment objective:**

The assessment covers:

- a functional sufficiency assessment of a confidentiality protecting communication mechanism used by the personal wearable to fulfil [CONF-COM] clause 5.8.2 for authentication level CONF.COM.Medium or CONF.COM.Enhanced.

based on the default configuration required by clause 5.4.1.

**Assessment preparation:**

The following documentation for the personal wearable shall be complete:

- for the confidentiality protecting communication mechanism used by the personal wearable to achieve CONF.COM.Medium or CONF.COM.Enhanced:
  - documentation of the measures to prevent the downgrade of the confidentiality protecting communication mechanisms protection level by communication endpoints.

The following test setups shall be prepared:

- a test setup to access the documented confidentiality protecting communication mechanism via a documented interface;
- a test setup to alter parameters of communication protocols, determining e.g. used protocol versions or cipher suites.

**Assessment activities:**

The following activities shall be performed:

- verify whether the confidentiality protecting communication mechanism refuses to send confidential data using communication protocol parameters that would result in a protection level below CONF.COM.Medium or CONF.COM.Enhanced respectively;

- verify whether the confidentiality protecting communication mechanism refuses alteration of communication protocol parameters that would result in a protection level below CONF.COM.Medium or CONF.COM.Enhanced during the communication of confidential data.

**Assessment verdict:**

The verdict PASS shall be assigned if:

- the confidentiality protecting communication mechanism refuses to send confidential data using communication protocol parameters that would result in a protection level below CONF.COM.Medium or CONF.COM.Enhanced respectively; and
- the confidentiality protecting communication mechanism refuses alteration of communication protocol parameters that would result in a protection level below CONF.COM.Medium or CONF.COM.Enhanced during the communication of confidential data.

The verdict FAIL shall be assigned otherwise.

**Assessment evidence:**

- all test records of the performed test.

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

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

- to develop products that are compliant to; or
- to analyse the compliance of a product to;

the present document.

- Step 1 - check if the product is in scope of the present document provided in clause 1 by:
  - verifying that the product meets the "technical description" of the "category of product" number "16." by Regulation (EU) 2025/2392 [i.2]; and
  - identifying the product context by:
    - identifying the product's architectural components; and
    - identifying all data processed by the product (data assets); and
    - identifying all functions provided by the product (function assets); and
    - identifying the architectural components' operational environments; and
    - identifying the architectural components' interfaces and communication types; and
  - verifying that the product is covered within the product context described in clause 4 by:
    - verifying that the architectural components of the product are covered within the product architecture described in clause 4.2; and
    - verifying that the data processed by the product and the functions provided by the product are covered within clause 4.1; and
    - verifying that the architectural components' operational environments are covered within clause 4.3; and
    - verifying that the architectural components' interfaces and communication types are covered within clause 4.3.4.

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

NOTE 2: If a product meets the "technical description" of the "category of product" number "19." by Regulation (EU) 2025/2392 [i.2] but is not covered within the product context described in clause 4, it is assumed that the product is not or not completely covered by the present document. In such cases informing ETSI Technical Committee Cyber Working Group for EUSR (CYBER-EUSR) via the Committee Support Staff might help to address those products in potential revisions of the present document.

- Step 2 - identify information to determine risk factors by:
  - identifying for each function provided by the product:
    - its impact classes according to clause D.2; and
    - the architectural components that perform the function; and
    - the communication types and the interfaces that can receive corresponding function trigger input; and
  - identifying for each data processed by the product:
    - its impact classes according to clause D.1;

        - the architectural components that persistently store the data; and
        - the architectural components that can communicate the data; and
        - the communication types and the interfaces over which the data is communicated.

- Step 3 - identify concrete requirements for and specific security measures/mitigations of the product that satisfy those requirements by:
    - for each requirement in clause 5:
        - identifying the requirements applicability by evaluating the requirement's potential preconditions and exceptions based on the product's properties; and
        - (for requirements that include assignment tables) identifying the required protection mechanisms' strengths (specified in Annex E) by evaluating the requirement's assignment table based on the product's properties determining the attack surface and impact parameters; and
        - identifying the specific security measures/mitigations that satisfy the requirement.

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

EXAMPLE: Authentication requirements prior to changes of a personal wearable configuration are different whether the changes can be made via a cloud application, accessible from adjacent or public networks, a GUI, accessible from the personal wearable's touchscreen, or a mobile application, accessible from the mobile device hosting it. All of these cases can be simultaneously present on the same personal wearable.

- Step 4 - assess the compliance of the product with the requirements in clause 5 by:
    - for each requirement in clause 5, performing the corresponding assessment for compliance described in clause 6 (the functional sufficiency assessments for different protection measures strengths are specified in Annex E) by:
        - preparing the assessment for the product; and
        - performing the assessment activities for the product; and
        - assigning an assessment verdict for the product; and
        - generating the supporting evidence for the assessment.

Figure F.1 provides a graphical representation of the guidance for the application of the present document.

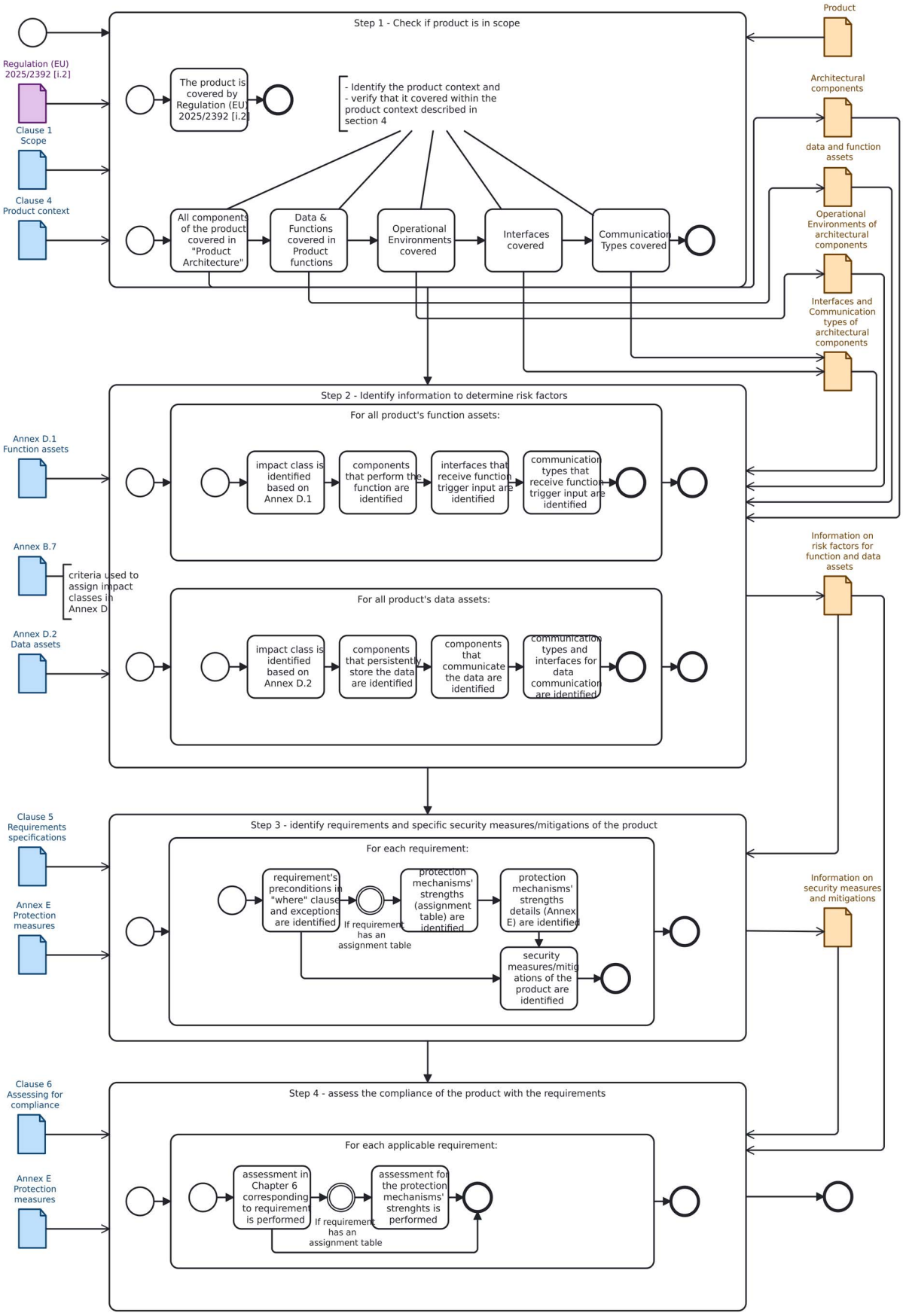


**Figure F.1: Graphical representation on guidance for the application of the present document**

# Annexes G to J:
# Void

# Annex K (normative): Generic requirements and assessment criteria for the use of state of the art cryptography

## K.1 Cryptography

### K.1.1 Requirement

The product's default configuration shall only use cryptographic mechanisms that meet at least one of the following criteria:

1) ACM-listed: the cryptographic mechanism is listed in the ECCG Agreed Cryptographic Mechanisms (ACM) catalogue [1];

2) ACM-extended: the cryptographic mechanism is not listed in the ECCG Agreed Cryptographic Mechanisms (ACM) catalogue [1] and meets at least one of the following conditions:

   a) the cryptographic mechanism is listed in clause K.3.2 as an ACM-extended cryptographic mechanism for the specific product function(s);

   b) where the cryptographic mechanism is not listed in clause K.3.2, the cryptographic mechanism meets all the following criteria:

      i. the cryptographic mechanism, or where applicable the ACM-listed cryptographic mechanism on which it is based, is not deprecated per the ECCG Agreed Cryptographic Mechanisms (ACM) catalogue [1];

      ii. the cryptographic mechanism has been specified, developed or maintained through a transparent process by a recognised European, international or sector-specific standards development organisation, or by an industry specification organisation accountable for the relevant specification*;* or the cryptographic mechanism is listed as suitable in a publicly available cryptographic catalogue maintained by a recognised national or governmental cybersecurity authority, where the catalogue is maintained under a documented revision and retirement process;

      iii. the cryptographic mechanism is described in a valid, publicly available and uniquely referenceable specification;

      iv. the cryptographic properties of the cryptographic mechanism are known;

      v. no known weakness affects the cryptographic mechanism in a way that affects its cryptographic properties;

      vi. the cryptographic mechanism is required for a specific set of product functions;

3) Interoperability-based: the cryptographic mechanism is listed in clause K.4.2 as an interoperability-based cryptographic mechanism for specific product function(s) and external specification(s) or external requirement(s).

NOTE 1: The reference to the product's default configuration is intended to define a clear and assessable baseline, corresponding to the configuration in which the product is placed on the market. The product can provide several configurations that fulfil the requirement.

NOTE 2: For products supplied as hardware platforms or components to be configured by an integrator, references in this annex to the product's default configuration refer to the configuration specified for the intended operational use of the product after integration, including the relevant integration assumptions and configuration constraints.

NOTE 3: The applicable ACM catalogue version is identified in the normative references of the present document. The lifecycle treatment of mechanisms affected by ACM deprecation dates, expiry dates, migration conditions or usage limitations is addressed in clause K.2.

NOTE 4: In this clause, an external specification or external requirement means a specification or requirement that is imposed on the product, and which requires the use of a specific cryptographic mechanism for the product to interoperate with an identified system, platform or operational context. An external requirement can be a regulatory requirement, operational constraint, technical interoperability constraint, or platform compatibility requirement.

NOTE 5: Inclusion of a cryptographic mechanism under the interoperability-based criterion does not classify that mechanism as state-of-the-art cryptography.

EXAMPLE: Examples of product functions include secure communication based on TLS 1.3; authenticated encryption of communicated data based on AES-GCM; storage confidentiality based on AES-XTS; firmware signature verification based on Ed25519; and key derivation based on HKDF.

# K.1.2 Assessment of product cryptographic configuration

## K.1.2.0 General

The assessment in clause K.1.2 verifies the cryptographic mechanisms used in the product's default configuration against clause K.1.1.

For ACM-extended cryptographic mechanisms, the assessment verifies that the cryptographic mechanism is either listed in clause K.3.2 or fulfils the criteria specified in clause K.1.1 item 2.b. For interoperability-based cryptographic mechanisms, the assessment verifies that the cryptographic mechanism is listed in clause K.4.2. The assessment also verifies that the product uses the cryptographic mechanism in accordance with the relevant characteristics, product functions, use cases where applicable, external specifications or external requirements, and conditions specified in the present document.

## K.1.2.1 Assessment of ACM-listed cryptographic mechanisms

### K.1.2.1.1 Assessment objective

The purpose of this assessment case is to verify that cryptographic mechanisms claimed to comply with clause K.1.1 item 1) and used in the product's default configuration are listed in the ECCG Agreed Cryptographic Mechanisms (ACM) catalogue [1].

### K.1.2.1.2 Assessment preparation

- Preconditions for the assessment: The product's default configuration shall be used for the assessment.
- The documentation shall provide a list of cryptographic mechanisms used in the product's default configuration and claimed under clause K.1.1 item 1), including the related product function, relevant parameters where applicable, and the relevant ACM entry.

### K.1.2.1.3 Assessment activities

The assessment shall include verification that:

a) each cryptographic mechanism claimed under clause K.1.1 item 1) is identified by reference to a relevant ACM entry;

b) the ACM entry corresponds to the cryptographic mechanism used in the product's default configuration, including relevant parameters where applicable;

c) where the ACM entry includes lifecycle information, such as expiry date, deprecation date, migration condition or usage limitation, this information is reflected in the documentation.

#### K.1.2.1.4 Assessment evidence

The assessment evidence shall include, as applicable:

a) description of the product's default configuration;

b) list of cryptographic mechanisms claimed under clause K.1.1 item 1);

c) references to the relevant ACM entries;

d) relevant parameters, profiles, cipher suites or configuration constraints, where applicable;

e) relevant lifecycle information from the ACM catalogue, where applicable.

#### K.1.2.1.5 Assessment verdict

- The verdict PASS shall be assigned if the required evidence has been provided, is complete, is applicable to the assessed configuration, and demonstrates compliance with clause K.1.1 item 1).
- The verdict FAIL shall be assigned otherwise.

### K.1.2.2 Assessment of ACM-extended cryptographic mechanisms

#### K.1.2.2.1 Assessment objective

The purpose of this assessment case is to verify that cryptographic mechanisms claimed to comply with clause K.1.1 item 2) and used in the product's default configuration are either listed as ACM-extended cryptographic mechanisms in clause K.3.2 or fulfil the criteria specified in clause K.1.1 item 2.b, and are used for the claimed product function(s).

#### K.1.2.2.2 Assessment preparation

- Preconditions for the assessment: The product's default configuration shall be used for the assessment.
- The documentation shall provide a list of cryptographic mechanisms used in the product's default configuration and claimed under clause K.1.1 item 2), including the related product function, use case where applicable, relevant parameters where applicable, and at least one of the following:

  a) the relevant entry in clause K.3.2; or

  b) evidence that the cryptographic mechanism fulfils all applicable criteria in clause K.1.1 item 2.b.

#### K.1.2.2.3 Assessment activities

The assessment shall include verification that:

a) each cryptographic mechanism claimed under clause K.1.1 item 2) is either listed in clause K.3.2 as an ACM-extended cryptographic mechanism or supported by evidence demonstrating fulfilment of the applicable criteria in clause K.1.1 item 2.b;

b) the cryptographic mechanism used by the product corresponds to the mechanism listed in clause K.3.2 or described in the evidence provided under clause K.1.1 item 2.b;

c) the product function using the cryptographic mechanism, and the use case where applicable, correspond to the related product function and use case specified in clause K.3.2 or justified under clause K.1.1 item 2.b;

d) the relevant characteristics, parameters, profiles, cipher suites or configuration constraints of the cryptographic mechanism correspond to those specified in clause K.3.2 or justified under clause K.1.1 item 2.b, where applicable;

e) where clause K.3.2 or the justification under clause K.1.1 item 2.b defines conditions or limitations for the use of the cryptographic mechanism, these conditions or limitations are reflected in the product's default configuration;

f) where technically feasible, the cryptographic mechanism, parameters and configuration identified in the documentation correspond to the assessed product configuration.

#### K.1.2.2.4 Assessment evidence

The assessment evidence shall include, as applicable:

a) description of the product's default configuration;

b) list of cryptographic mechanisms claimed under clause K.1.1 item 2);

c) reference to the relevant entry in clause K.3.2, where the mechanism is listed in clause K.3.2;

d) evidence that the cryptographic mechanism fulfils the criteria in clause K.1.1 item 2.b, where compliance with clause K.1.1 item 2 is claimed on the basis of those criteria;

e) identification of the related product function using the cryptographic mechanism and the use case where applicable;

f) relevant characteristics, parameters, profiles, cipher suites or configuration constraints, where applicable;

g) evidence that the cryptographic mechanism is used in accordance with the conditions or limitations specified in clause K.3.2 or in the justification under clause K.1.1 item 2.b, where applicable.

#### K.1.2.2.5 Assessment verdict

- The verdict PASS shall be assigned if the required evidence has been provided, is complete, is applicable to the assessed configuration, and demonstrates compliance with clause K.1.1 item 2).
- The verdict FAIL shall be assigned otherwise.

### K.1.2.3 Assessment of interoperability-based cryptographic mechanisms

#### K.1.2.3.1 Assessment objective

The purpose of this assessment case is to verify that cryptographic mechanisms claimed to comply with clause K.1.1 item 3) and used in the product's default configuration are listed as interoperability-based cryptographic mechanisms in clause K.4.2 and are used in accordance with the characteristics, product functions, use cases where applicable, external specifications or external requirements, and conditions specified in clause K.4.2.

#### K.1.2.3.2 Assessment preparation

- Preconditions for the assessment: The product's default configuration shall be used for the assessment.
- The documentation shall provide a list of cryptographic mechanisms used in the product's default configuration and claimed under clause K.1.1 item 3), including the related product function, use case where applicable, relevant parameters where applicable, the external specification or external requirement requiring its use, and the relevant entry in clause K.4.2.

#### K.1.2.3.3 Assessment activities

The assessment shall include verification that:

a) each cryptographic mechanism claimed under clause K.1.1 item 3) is listed in clause K.4.2 as an interoperability-based cryptographic mechanism;

b) the cryptographic mechanism used by the product corresponds to the cryptographic mechanism listed in clause K.4.2;

c) the product function using the cryptographic mechanism, and the use case where applicable, correspond to the related product function and use case specified in clause K.4.2;

d) the external specification or external requirement requiring the use of the cryptographic mechanism corresponds to the external specification or external requirement specified in clause K.4.2;

e) the relevant characteristics, parameters, profiles, cipher suites or configuration constraints of the cryptographic mechanism correspond to those specified in clause K.4.2, where applicable;

f) the conditions or limitations specified in clause K.4.2 for the use of the cryptographic mechanism are reflected in the product's default configuration;

g) where technically feasible, the cryptographic mechanism, parameters and configuration identified in the documentation correspond to the assessed product configuration.

#### K.1.2.3.4 Assessment evidence

The assessment evidence shall include, as applicable:

a) list of cryptographic mechanisms claimed under clause K.1.1 item 3);

b) list of cryptographic mechanisms claimed under clause K.1.1 item 3);

c) reference to the relevant entry in clause K.4.2;

d) identification of the related product function using the cryptographic mechanism and the use case where applicable;

e) identification of the external specification or external requirement requiring use of the cryptographic mechanism;

f) relevant characteristics, parameters, profiles, cipher suites or configuration constraints, where applicable;

g) evidence that the cryptographic mechanism is used in accordance with the conditions or limitations specified in clause K.4.2.

#### K.1.2.3.5 Assessment verdict

- The verdict PASS shall be assigned if the required evidence has been provided, is complete, is applicable to the assessed configuration, and demonstrates compliance with clause K.1.1 item 3).
- The verdict FAIL shall be assigned otherwise.

NOTE 1: The assessment of the external specification or external requirement itself is outside the scope of this assessment case. The assessment verifies that the external specification or external requirement is identified in clause K.4.2 and that the cryptographic mechanism is used by the product for the related product function.

NOTE 2: Documentation review is a minimum assessment activity under the present annex. Functional and/or resistance testing activities can be added by vertical standards where relevant for the product category, product function or cryptographic mechanism.

## K.2 Crypto agility

### K.2.1 Requirement

Where the product's default configuration uses a cryptographic mechanism for which the ACM catalogue, or the present document, specifies a deprecation date, expiry date, migration condition or usage limitation falling within the intended lifetime of the product, the product shall provide means for addressing the affected cryptographic mechanism by one or more of the following:

a) updating the cryptographic mechanism;

b) using another cryptographic mechanism that complies with clause K.1.1 and is not subject to the relevant deprecation date, expiry date, migration condition or usage limitation;

c) disabling the use of the affected cryptographic mechanism; or

d) limiting the use of the affected product functions accordingly.

EXAMPLE: Where a security mechanism uses a hybrid cryptographic construction, for example a hybrid key-encapsulation mechanism combining a classical and a post-quantum primitive, the lifecycle status of each constituent primitive is relevant to the lifecycle status of the construction. Hybridisation can be used as part of a planned migration strategy where permitted by the ACM catalogue or by the present document. However, hybridisation does not, by itself, extend the recommended usage lifetime of a constituent primitive that has been deprecated.

NOTE 1: Where a hybrid cryptographic construction includes multiple cryptographic primitives, the lifecycle status of each constituent primitive is relevant to the lifecycle status of the construction. Hybridisation is not assumed to mitigate the deprecation of a constituent primitive unless the ACM catalogue or the present document classifies the hybrid construction as suitable for the corresponding product function.

NOTE 2: Crypto agility supports maintaining appropriate cryptographic protection within the intended lifetime of the product, in addition to the capability of updating cryptographic mechanisms on the product in accordance with secure update and secure communication mechanisms.

NOTE 3: Deprecation information from sources other than the ACM catalogue or the present document can be considered as input to vulnerability management or security risk assessment but does not by itself trigger the requirement in clause K.2.1.

NOTE 4: Where the product provides cryptographic capabilities for use by other products, components or layers, the mechanism required by clause K.2.1 can consist of update, configuration, disabling, deprecation or limitation capabilities usable by the integrating product, system operator or user, where applicable.

NOTE 5: The applicability condition of this requirement can express exceptions based on product characteristics, e.g. cryptographic implementation based on immutable hardware co-processor(s) or hardware-based root of trust, or long-lived silicon used in a long-lived non-updateable environment.

## K.2.2 Assessment of crypto-agility

### K.2.2.1 Assessment objective

The purpose of this assessment case is to verify whether, where the product's default configuration uses a cryptographic mechanism for which the ACM catalogue, or the present document, specifies a deprecation date, expiry date, migration condition or usage limitation falling within the intended lifetime of the product, the product provides means to address the affected cryptographic mechanism in accordance with clause K.2.1.

### K.2.2.2 Assessment preparation

- Preconditions for the assessment: The product's default configuration shall be used for the assessment.
- The documentation shall identify:

  a) the intended lifetime of the product;

  b) the cryptographic mechanisms used in the product's default configuration;

  c) the related product function(s) for each cryptographic mechanism;

  d) the lifecycle information applicable to each cryptographic mechanism, where specified by the ACM catalogue or the present document, including any deprecation date, expiry date, migration condition or usage limitation.

### K.2.2.3 Assessment activities

The assessment shall include verification that:

a) for each cryptographic mechanism used in the product's default configuration, the lifecycle information specified by the ACM catalogue or the present document has been identified, where such information is specified;

b) where the ACM catalogue or the present document specifies a deprecation date, expiry date, migration condition or usage limitation for a cryptographic mechanism, this information is reflected in the documentation;

c) where a deprecation date, expiry date, migration condition or usage limitation falls within the intended lifetime of the product, the product provides an applicable mechanism for updating the cryptographic mechanism, using another cryptographic mechanism that complies with clause K.1.1 and is not subject to the relevant deprecation date, expiry date, migration condition or usage limitation, disabling the use of the affected cryptographic mechanism, or limiting the use of the affected product functions accordingly;

d) where another cryptographic mechanism is used, that cryptographic mechanism complies with clause K.1.1 and is not subject to the relevant deprecation date, expiry date, migration condition or usage limitation.

### K.2.2.4 Assessment evidence

The assessment evidence shall include, as applicable:

a) documentation of the intended lifetime of the product;

b) list of cryptographic mechanisms used in the product's default configuration;

c) identification of the related product function(s) for each cryptographic mechanism;

d) references to the ACM catalogue entry or to the provision of the present document used to determine lifecycle information, where applicable;

e) identification of any deprecation date, expiry date, migration condition or usage limitation falling within the intended lifetime of the product;

f) description of the means provided by the product, such as update of the cryptographic mechanism, use of another cryptographic mechanism that complies with clause K.1.1 and is not subject to the relevant lifecycle constraint, disabling the use of the affected cryptographic mechanism, or limitation of the use of the affected product functions.

### K.2.2.5 Assessment verdict

- The verdict PASS shall be assigned if the required evidence has been provided, is complete, is applicable to the assessed configuration, and demonstrates compliance with clause K.2.1.
- The verdict FAIL shall be assigned otherwise.

## K.3 ACM-extended cryptographic mechanisms

### K.3.1 Requirement

Where the product's default configuration uses ACM-extended cryptographic mechanisms, these mechanisms shall comply with the ACM-extended criterion in clause K.1.1 item 2.

### K.3.2 List of ACM-extended cryptographic mechanisms

Table K.1 lists the ACM-extended cryptographic mechanisms specified by the present document.

**Table K.1: ACM-extended cryptographic mechanisms**

| ACM-extended cryptographic mechanism | Type of cryptographic mechanism | Characteristics / parameters | Related product function(s) / use case(s), where applicable | Cryptographic properties | Specification / reference | Conditions or limitations, where applicable |
|---|---|---|---|---|---|---|
| <mechanism name> | <Algorithm / Primitive / Scheme / Protocol / Protocol profile / Cipher suite / Mode / Construction / Parameter set / Other> | <key length, mode, profile, cipher suite, parameter set, version, etc.> | <product function, interface, protocol context, operational context, etc.> | <confidentiality, integrity, authentication, key establishment, etc.> | <publicly available and uniquely referenceable specification> | <constraints, permitted use, excluded use, configuration limitation, lifecycle limitation, etc.> |

### K.3.3 Assessment

Compliance with the ACM-extended criterion in clause K.1.1 item 2 is assessed in clause K.1.2.2.

## K.4 Interoperability-based cryptographic mechanisms

### K.4.1 Requirement

Where the product's default configuration uses interoperability-based cryptographic mechanisms, these mechanisms shall be selected from the interoperability-based cryptographic mechanisms listed in clause K.4.2 for the specified product functions and external specifications or external requirements and shall be used in accordance with the conditions or limitations specified in clause K.4.2.

### K.4.2 List of interoperability-based cryptographic mechanisms

Table K.2 lists the interoperability-based cryptographic mechanisms specified by the present document.

**Table K.2: Interoperability-based cryptographic mechanisms**

| Interoperability-based cryptographic mechanism | Type of cryptographic mechanism | Characteristics / parameters | Related product function(s) / use case(s), where applicable | External specification(s) or external requirement(s) | Interoperability justification | Conditions or limitations, where applicable |
|---|---|---|---|---|---|---|
| <mechanism name> | <Algorithm / Primitive / Scheme / Protocol / Protocol profile / Cipher suite / Mode / Construction / Parameter set / Other> | <key length, mode, profile, cipher suite, parameter set, version, etc.> | <product function, interface, protocol context, operational context, etc.> | <external specification, regulatory requirement, mandatory public-sector requirement, operational constraint requiring use of the mechanism, technical interoperability constraint, platform compatibility requirement, etc.> | <why the mechanism is needed for interoperability> | <constraints, permitted use, excluded use, negotiation preference, external system or requirement, compensating measures, migration expectation, warning/logging, lifecycle limitation, etc.> |

## K.4.3 Assessment

Compliance with the requirement in clause K.4.1 is assessed in clause K.1.2.3.

NOTE: The assessment of the external specifications or external requirements themselves is outside the scope of this assessment. Their relevance is deemed confirmed by their inclusion in the present document.

# Annexes L to Q:
# Void

# Annex R (informative): Guidance on RDPS

The clause 4.2 specifies the architectural component that can form a personal wearable in scope of the present document. RDPS are typically software architectural components and in scope of the present document. The requirements specified in clause 5 are formulated such that they apply, where relevant, for RDPS.

For example:

- [ACM-FH] and [AUM-FH] address access control and authentication for functions whose use can cause harm, which can be provided by RDPSs;
- [CONF-COM] and [INT-COM] address confidentiality and integrity of communicated data, which can be communicated from or to RDPSs;
- [CONF-SSM] and [INT-SSM] address confidentiality and integrity of persistently stored data, which can be persistently stored on RDPSs;
- [AVAI-TIME-OUTA-NOT] addresses a defined behaviour when time sensitive functions, which can be provided by RDPSs, become or are unavailable;
- [AVAI-TIME-RECO-NETW] addresses the behaviour when a reconnection happens after the loss of network connection, which could happen for a RDPS.

# Annex S (informative): Change history

| Version | Information about changes |
|---|---|
| 0.0.1 | Early draft |
| 0.0.2 | Early draft presented the 2nd September 2025 |
| 0.1.0 | Stable draft uploaded the 5th December 2025 |
| 0.2.0 | Mature draft presented the 27th January 2026 |
| 0.2.2 | Editorial changes |
| 0.2.3 | Sent to editHelp |
| 0.2.4 | Finalised for HASC assessment |
| 0.3.0 | Final draft presented the 15th June 2026 |

# History

| Version | Date | Status | |
|---|---|---|---|
| V1.0.0 | July 2026 | SRdAP process | EV 20261015: 2026-07-23 to 2026-10-15 |
| | | | |
| | | | |
| | | | |
| | | | |