Draft ETSI EN 304 632 V1.0.0 (2026-07)

HARMONISED EUROPEAN STANDARD

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

Reference
DEN/CYBER-EUS-0014

Keywords
CRA, cybersecurity, intelligent homes & buildings

ETSI

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

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

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

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

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

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

Modal verbs terminology

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

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

Introduction

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

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

1 Scope

The present document specifies vulnerability handling activities, technical requirements and corresponding assessment criteria for smart home products with security functionalities related to cybersecurity. The products with digital elements in scope, thereafter "smart home products with security functionalities":

- are specified within the "technical description" of the "category of product" number "17." by the Commission Implementing Regulation (EU) 2025/2392 [i.2] as:
  "Products with digital elements that protect the physical security of consumers in a residential setting and which can be controlled or managed remotely from other systems, as well as hardware and software that centrally control such products.
  This category includes but is not limited to smart door locking devices, baby monitoring systems, alarm systems and home security cameras"; and

- are only covered within the product context described in clause 4.

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

2 References

2.1 Normative references

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

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

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

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

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

2.2 Informative references

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

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

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

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

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

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

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

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

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

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

[i.6] ETSI EN 304 623 (V1.1.1): "Cyber Security (CYBER); CRA; Cybersecurity requirements for boot managers".

[i.7] ISO/IEC 24760-1:2025: "Information security, cybersecurity and privacy protection - A framework for identity management - Part 1: Core concepts and terminology".

[i.8] ETSI TS 103 732-2 (V1.1.1): "CYBER; Consumer Mobile Device; Part 2: Biometric Authentication Protection Profile Module".

[i.9] NIST SP 800-78-5: ""Cryptographic Algorithms and Key Sizes for Personal Identity Verification".

[i.10] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[i.11] IETF RFC 8613: "Object Security for Constrained RESTful Environments (OSCORE)".

[i.12] IETF RFC 9528: "Ephemeral Diffie-Hellman Over COSE (EDHOC)".

[i.13] IETF RFC 9147: "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3".

[i.14] IEC 62820-1-1:2026: "Building intercom systems - Part 1-1: System requirements - General".

[i.15] IEC 62820-1-2:2017: "Building intercom systems - Part 1-2: System requirements - Building intercom systems using the internet protocol (IP)".

[i.16] IEC 62820-2:2017: "Building intercom systems - Part 2: Requirements for advanced security building intercom systems (ASBIS)".

[i.17] IEC 62820-3-1:2017: "Building intercom systems - Part 3-1: Application guidelines - General".

[i.18] IEC 62820-3-2:2018: "Building intercom systems - Part 3-2: Application guidelines - Advanced security building intercom systems (ASBIS)".

[i.19] EN 14604: "Smoke alarm devices" produced by CEN CENELEC.

[i.20] BS 5446-2:2003: "Fire detection and fire alarm devices for dwellings Specification for heat alarms".

[i.21] EN 50291-1: "Gas detectors - Electrical apparatus for the detection of carbon monoxide in domestic premises - Part 1: Test methods and performance requirements" produced by CEN CENELEC.

[i.22] EN 50194-1: "Electrical apparatus for the detection of flammable gases in household premises - Part 1: Test methods and performance requirements" produced by CEN CENELEC.

[i.23] EN 50131-1: "Alarm systems - Intrusion and hold-up systems - System requirements" produced by CEN CENELEC.

[i.24] EN 50131-2-2: "Alarm systems - Intrusion and hold-up systems - Requirements for passive infrared detectors" produced by CEN CENELEC.

[i.25] EN 50131-2-3: "Alarm systems - Intrusion and hold-up systems - Requirements for microwave detectors" produced by CEN CENELEC.

[i.26] EN 50131-2-4: "Alarm systems - Intrusion and hold-up systems - Requirements for combined passive infrared and microwave detectors" produced by CEN CENELEC.

[i.27] EN 50131-2-5: "Alarm systems - Intrusion and hold-up systems - Requirements for combined passive infrared and ultrasonic detectors" produced by CEN CENELEC.

[i.28] EN 50131-2-6: "Alarm systems - Intrusion and hold-up systems - Opening contacts (magnetic)" produced by CEN CENELEC.

[i.29] EN 50131-2-7-1: "Alarm systems - Intrusion and hold-up systems - Intrusion detectors - Glass break detectors (acoustic)" produced by CEN CENELEC.

[i.30] EN 50131-2-7-2: "Alarm systems - Intrusion and hold-up systems - Intrusion detectors - Glass break detectors (passive)" produced by CEN CENELEC.

[i.31] EN 50131-2-7-3: "Alarm systems - Intrusion and hold-up systems - Intrusion detectors - Glass break detectors (active)" produced by CEN CENELEC.

[i.32] EN 50131-2-8: "Alarm systems - Intrusion and hold-up systems - Intrusion detectors - Shock detectors" produced by CEN CENELEC.

[i.33] EN 50131-2-10: "Alarm systems - Intrusion and hold-up systems - Intrusion detectors - Lock state contacts (magnetic)" produced by CEN CENELEC.

[i.34] EN 50131-3: "Alarm systems - Intrusion and hold-up systems - Control and indicating equipment" produced by CEN CENELEC.

[i.35] EN 50131-4: "Alarm systems - Intrusion and hold-up systems - Warning devices" produced by CEN CENELEC.

[i.36] EN 50131-5-3: "Alarm systems - Intrusion systems - Requirements for interconnections equipment using radio frequency techniques" produced by CEN CENELEC.

[i.37] EN 50131-6: "Alarm systems - Intrusion and hold-up systems - Power supplies" produced by CEN CENELEC.

[i.38] EN 50131-8: "Alarm systems - Intrusion and hold-up systems - Security fog devices" produced by CEN CENELEC.

[i.39] EN 50131-10: "Alarm systems - Intrusion and hold-up systems - Application specific requirements for Supervised Premises Transceiver (SPT)" produced by CEN CENELEC.

[i.40] EN 50131-13: "Alarm systems - Intrusion and hold-up systems - Pyrotechnic Obscuration Security Devices" produced by CEN CENELEC.

[i.41] EN 50134-1: "Alarm systems - Social alarm systems - System requirements" produced by CEN CENELEC.

[i.42] EN 50134-2: "Alarm systems - Social alarm systems - Trigger devices" produced by CEN CENELEC.

[i.43] EN 50134-3: "Alarm systems - Social alarm systems - Local unit and controller" produced by CEN CENELEC.

[i.44] EN 50134-5: "Alarm systems - Social alarm systems - Interconnections and communications" produced by CEN CENELEC.

[i.45] EN 50134-7: "Alarm systems - Social alarm systems - Application guidelines" produced by CEN CENELEC.

[i.46] NIST FIPS 203: "Module-Lattice-Based Key-Encapsulation Mechanism Standard".

[i.47] NIST FIPS 204: "Module-Lattice-Based Digital Signature Standard".

[i.48] NIST SP 800-57-1: "Recommendation for Key Management: Part 1 - General".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

3.1.1 Architecture related terms

application software: software designed to perform specific user- or SHPSF-oriented functional tasks on a device, operating on top of the core software, and without direct responsibility for hardware initialization or fundamental system control

EXAMPLE: A mobile app, desktop software or parts of architectural component's embedded software that implements essential functionalities.

NOTE: Application software typically uses APIs provided by core software.

architectural component: self-contained hardware architectural component or software architectural component that is part of the SHPSF

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

EXAMPLE: A hardware architectural component's operating system, hardware abstraction layer or APIs for application software.

hardware architectural component: self-contained hardware part of the SHPSF including its associated software architectural component

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

EXAMPLE: Companion-App, RDPS-Cloud-Application.

3.1.2 Asset categories

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

data asset: asset, that is data processed by the SHPSF

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

function whose use can cause harm:

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

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

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

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

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

3.1.3 Communication types

adjacent communication: ingoing/outgoing communication from/to private networks which does not require physical proximity to the communication partner

EXAMPLE: Communication through a virtual-private-network tunnel with a communication partner in a private network.

local communication: ingoing/outgoing communication which requires physical proximity to but not physical presence at the communication partner

EXAMPLE 1: Point to point communication via short-range wireless technologies between two communication partners.

EXAMPLE 2: Radio communication between components of an alarm system or between alarm devices.

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

EXAMPLE 1: Communication via internet.

EXAMPLE 2: Alarm transmission through a public network.

strict local communication: ingoing/outgoing communication which requires physical presence at the communication partner

EXAMPLE 1: Communication with a hardware architectural component via its key-pad.

EXAMPLE 2: Communication between a RF tag and tag reader of an alarm system.

3.1.4 Data assets

actuator control data: data asset intended to control an actuator function

audit event data: data asset that contains information produced by monitoring mechanisms that can be used by logging mechanisms

NOTE 1: Typically contains records of events relevant for the cybersecurity of the SHPSF, its connected networks and other devices.

NOTE 2: Audit event data are typically user-related data.

authorisation policy data: data asset that contains an authorisation policy

EXAMPLE: Assignment of privileges to users.

battery status data: data asset that represents the charge level of a device

cryptographic security parameter: data asset that determines the cryptographic operations of a cryptographic function

EXAMPLE: Passwords, data hashes, message authentication codes, keys used for symmetric or asymmetric cryptography, (pseudo-)random numbers.

device identifier data: data asset the identifies a specific device

entity's location data: data asset that is not public data and represents the location/position of an entity

NOTE: Entity including but not limited to user and architectural component.

fire detection data: data asset that indicates the presence of a fire

EXAMPLE: Sensor data for physical parameters related to a fire such as temperature distributions or photoelectrical signals (detecting smoke).

function binary data: data asset stored on the SHPSF that implements the logic of a SHPSF's function asset.

function configuration data: data asset intended to configure a function asset

function fault detection data: data asset that indicates a detected fault of a function provided by a device or system

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

hold-up detection data: data asset contains the time and type of a specific hold up event

human emergency detection data: data asset that indicates whether a human is in an emergency situation and might need help

identity data for authentication: data asset that contains identity information and that is not a cryptographic security parameter and used for authentication

EXAMPLE: Data containing user/device identifier.

inflammable/explosive gas detection data: data asset that indicates the presence of an inflammable or explosive gas

EXAMPLE: Sensor data for physical parameter related to inflammable or explosive gases such as infrared absorption.

intrusion detection data: data asset that indicates the presence or an attempted intrusion of a being in supervised premises

locking element position data: data asset that represents the physical position or state of the locking element of a lock

EXAMPLE: Data representing the position of bolt, latch or related to a comparable mechanism.

logging data: data asset that contains information logged by logging mechanisms

network status data: data asset that describes an architectural component's network connections status

object tamper detection data: data asset that indicates whether an object is tampered

other products' function configuration data: data asset intended to configure other products' functions

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

personal notes data: data asset that represents personal information where the content is not specified by the manufacturer but can be freely filled by the user

private audio data: data asset that is not public data and represents audio information

EXAMPLE 1: Audio data recorded by the SHPSF.

EXAMPLE 2: Audio data provided by the user.

NOTE: Private audio data does not include publicly accessible audio recordings from the internet.

private video data: data asset that is not public data and represents video information

EXAMPLE 1: Video or picture recordings processed (including storage) by the SHPSF.

EXAMPLE 2: Video data provided by the user.

NOTE: Private video data does not include publicly accessible videos from the internet.

public data asset: data asset derived from public data

real-time data: data asset which represents (current) time and date

NOTE: Typically used for security specific processing, logging and communication (e.g. secure time validation such as certificate date validation, time of an intrusion/hold-up event, time synchronization).

SHPSF tamper detection data: data asset that indicates whether an architectural component is tampered

software package: data asset that contains software intended to be installed on the SHPSF

state data: data asset that contains SHPSF state information

window/door opening status data: data asset that indicates whether a window or door is or has been opened, closed, locked or unlocked

3.1.5 Data related terms

authentication factor: element used by an entity to proof an identity claim

EXAMPLE: A PIN, a password, a fingerprint, a shared symmetric cryptographic key, an one-time-password generated by a security token, an one-time-password received by E-Mail.

NOTE: An authentication factor can be of the type knowledge, inherence or possession.

confidential cryptographic key: confidential data that is not an initialization vector or password which is used in the operation of a cryptographic function

EXAMPLE: Symmetric keys, private keys.

NOTE: A confidential cryptographic key is a cryptographic security parameter.

connection data: communicated data that contains information necessary for testing or establishing communication capability via machine interfaces

EXAMPLE: IP address as part of an IP package header.

data: information in digital form

derived token: short term authentication factor generated with the use of a security token

EXAMPLE: A time-based one-time secret which can be used to authenticate an entity, a response to a challenge which can be used authenticate an entity, a HMAC-based one-time password.

NOTE: Derived tokens can be provided by Services or via Accounts in possession of the entity or generated by a security token.

location data: data containing geographical information

password: sequence of characters used to authenticate an entity that is intended to be used by humans as an authentication factor of type knowledge

EXAMPLE: Symmetric keys, private keys.

NOTE 1: A password is a cryptographic security parameter.

NOTE 2: Passwords are sometimes chosen to be remembered by humans such as 4-digit PINs.

NOTE 3: Passwords are sometimes chosen to be complex e.g. when generated by a password manager under a respective configuration.

processed data: data processed by the SHPSF, including but not limited to capturing, storing, transmitting, modifying, deleting and presenting data

public data: data from publicly accessible sources

security token: long term authentication factor of the type possession

EXAMPLE: A private key which can be used authenticate an entity, a smartcard that can be used authenticate an entity, a long term symmetric key that can be used authenticate an entity.

targeted modification of stored data: physical modification of data storage that leads to a fully controlled change of the stored data

EXAMPLE: Physical overwrite of storage that stores a user password's reference value with a reference value for a password generated by an attacker.

user-related data: data provided by a user and/or about a user

3.1.6 Function assets

actuator control function: SHPSF function intended to control an actuator function

connection function: SHPSF function that is used for testing or establishing communication capability via machine interfaces

EXAMPLE 1: ICMP, DHCP Discovery.

EXAMPLE 2: SHPSF function for establishing the connection for remote access or remote alarm transmission.

NOTE: In this context, establishing communication means communication without user-related data and without authentication of the communication partner for the purpose of establishment of a connection.

data communication function: SHPSF function that communicates data assets to or receives data assets from another architectural component or another product

EXAMPLE: Video/audio intercom functions of a building intercom system e.g. based on a call through agenda, emergency calls of a social alarm system or intrusion/hold-up alarm system.

data modification function: SHPSF function that can create, delete or change data assets

EXAMPLE: Storing data created by an external sensing function.

data presenting function: SHPSF function that grants an entity read access to data or presents data to a user via physical human interface

EXAMPLE 1: Presenting data to a user on a website associated with a RDPS.

EXAMPLE 2: Presenting data on a display, controlling indicator lights.

external sensing function: SHPSF function to measure characteristics of its physical operational environment

EXAMPLE: Recording video or audio or measuring temperature, pressure or brightness.

fire/gas alarm function: SHPSF actuator function that alarms the presence of a fire or inflammable/explosive gas hazard in supervised premises

internal sensing function: SHPSF function to measure characteristics of the SHPSF or parts of it

EXAMPLE: Monitoring unsuccessful authentication attempts.

intrusion and hold up alarm function: SHPSF actuator function that alarms:

- at presence, entry or attempted entry of an intruder into supervised premises; and/or
- when a user deliberately generates a hold-up alarm condition

other products' configuration function: SHPSF function that allows to change the configuration of other product's functions

physical security notification function: SHPSF actuator function that notifies users in hazardous situations

EXAMPLE: Function that controls the sounder of a smoke alarm device.

power supply function: SHPSF actuator function that supplies power to hardware architectural components

EXAMPLE: The power supply equipment that supplies power to components of an alarm system.

security function: SHPSF function that protects SHPSF assets

EXAMPLE: Authentication mechanism, integrity protecting secure storage mechanism or input validation mechanism.

SHPSF basic protection object lock function: SHPSF actuator function that can change the securement state of a locking mechanism that is intended to control access to low value objects outside or inside a residence.

NOTE: Such functions can include opening/closing a simple padlock.

SHPSF exterior lock function: SHPSF actuator function that can change the securement state of a locking mechanism that is intended to control access from outside a residence to the inside.

NOTE: Such functions can include opening/closing the door of a resident's house or apartment.

SHPSF high protection object lock function: SHPSF actuator function that can change the securement state of a locking mechanism that is intended to control access to high value objects outside or inside a residence.

NOTE: Such functions can include opening/closing a vault.

SHPSF interior lock function: SHPSF actuator function that can change the securement state of a locking mechanism that is intended to control access within a residence.

NOTE: Such functions can include opening/closing the door within a resident's house or apartment.

SHPSF medium protection object lock function: SHPSF actuator function that can change the securement state of a locking mechanism that is intended to control access to medium value objects outside or inside a residence.

NOTE: Such functions can include opening/closing a physical protected mailbox lock or garden cabin lock.

social alarm function: SHPSF function that alarms when the user may need urgent help

3.1.7 Function related terms

access control mechanism: function that enforces an authorisation policy

NOTE: An access control mechanism is a security function.

actuator function: function that performs an action on the physical operational environment

authentication mechanism: function that verifies an entity's identity claim by using authentication factors of the type inherence, knowledge or possession.

NOTE: A authentication mechanism is a security function.

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

automated security update: a software security update that does not require an explicit trigger by a user

EXAMPLE 1: An update is automatically downloaded from the internet, verified and installed without user interaction when an internet connection is available.

EXAMPLE 2: A hardware architectural component with only local communication capabilities receives the update from another architectural component in its proximity. The other architectural component has a connection to the internet and downloads the software for the hardware architectural component without user interaction. The hardware architectural component is can only be automatically updated when the other architectural component is in its proximity.

bootloader function: function that initiates the execution of other core software at start up.

NOTE: A bootloader function is a security function.

confidentiality protecting communication mechanism: function that protects the confidentiality of communicated data

NOTE: A confidentiality protecting communication mechanism is a security function.

confidentiality protecting secure storage mechanism: function that protects the confidentiality of persistently stored data

NOTE: A confidentiality protecting secure storage mechanism is a security function.

configuration function: function that allows to change the configuration of SHPSF's functions

NOTE: A configuration function is a data modification function that modifies function configuration data.

cryptographic algorithm: sequence of instructions based on mathematical properties to protect confidentiality, integrity or authenticity against attackers.

NOTE: Cryptographic algorithms include cryptographic protocols/schemes/constructors/primes such as TLS/ Symmetric Entity Authentication Schemes/AES-128 as part of a CMAC/AES-256.

cryptographic function: function that performs cryptographic algorithm

NOTE: A cryptographic function is a security function.

cryptographic mechanism: security-related procedure using cryptography

NOTE 1: The term "cryptographic mechanism" is used as an umbrella term covering the categories used in the Agreed Cryptographic Mechanisms [1], 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 Agreed Cryptographic Mechanisms [1].

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 parameter guessing probability: probability of randomly guessing a valid authentication factor based on the expected number of guesses, the number of possible authentication factors and the number of valid authentication factors

EXAMPLE: For T_{SI} of one day (86 400 seconds), $C_{CP,min}$ of 10 000, only one valid combination at any time and $f_{VA,max}$ of $\frac{3}{3\times3s+3\,600s}$ for a waiting period of one hour after 3 failed attempts and 3 seconds per attempt, the $p_{GRP} = \frac{86\,400s\times3}{(3\times3+3\,600)s\times10\,000} \approx 7{,}18 \times 10^{-3}$.

NOTE: The p_{GRP} is defined in a way to allow for a tradeoff between complexity of passwords or PINs and restrictions on the number of attempts to enter a password or PIN.

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 backup mechanism: function that copies data assets to persistent storage of another architectural component or target outside the SHPSF.

NOTE: A data backup mechanism can be a data modification function and/or a data communication function.

data export mechanism: function that exports data assets for persistent storage in another device

NOTE: A data export mechanism can be a data presenting function and/or a data communication function.

data transfer mechanism: function that transfers data assets for persistent storage in another SHPSF's architectural component or in another device/service

NOTE: A data transfer mechanism is a data communication function.

effective cryptographic security parameter bitlength: base two logarithm of the maximum number of operations to break a cryptographic security parameter security property by brute-force-attacks.

EXAMPLE 1: $L_{CP,eff}$ is 192 for a 192-bit perfectly random AES key.

EXAMPLE 2: The $L_{CP,eff}$ is 256/2 = 128 for a perfectly random 256-bit Elliptic Curve Cryptography (ECC) key.

EXAMPLE 3: The $L_{CP,eff}$ is $0{,}0235 \times (\log_2(7\,680))^{3{,}54} \approx 201 > 192$ for a perfectly random 7 680-bit RSA key.

EXAMPLE 4: ML-KEM-512 has $L_{CP,eff}$ of 128 (security category 1, NIST FIPS 203 [i.46]) and ML-DSA-44 has $L_{CP,eff}$ of at least 128 (security category 1 or 2, NIST FIPS 204 [i.47]).

NOTE: Here, the $L_{CP,eff}$ is equal to the key length for perfectly random symmetric cryptographic keys, the half of key length for perfectly random asymmetric cryptographic keys based on Elliptic Curve Cryptography (ECC) and $L_{CP,eff} = 0{,}0236 \times (\log_2(key\ length))^{3{,}54}$ for perfectly random asymmetric cryptographic keys for RSA (Rivest-Shamir-Adleman) cryptosystems. The calculation of $L_{CP,eff}$ is based on the recommendations in NIST SP 800-78-5 [i.9]. For ML-KEM and ML-DSA, $L_{CP,eff}$ can be adapted form the "security category", see "security strength" in NIST SP 800-57-1 [i.48], with "security category 1" corresponding to an $L_{CP,eff}$ of 128, "security category 2" corresponding to an $L_{CP,eff}$ of 192 etc.

factory reset function: function that removes all user-related data and sets the architectural components in a factory default state, potentially keeping software updates

NOTE: A factory reset function is a data modification function.

false acceptance rate: frequency at which an unknown entity is incorrectly accepted by an authentication mechanism

NOTE: The FAR is a parameter used to differentiate between authentication strength levels in clause E.1.

false rejection rate: frequency at which an known identity is incorrectly rejected by an authentication mechanism

NOTE: The FRR is a parameter used to differentiate between authentication strength levels in clause E.1.

function output: output of an architectural component's functions that is:

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

NOTE: Function output that is an action on the physical operational environment can be performed by a SHPSF's actuator function.

function trigger input: input to an architectural component's functions provided by:

- human users,
- devices or services, or
- the physical operational environment

NOTE: Function trigger input provided by the physical operational environment can be received by a SHPSF's external sensing function.

identity: set of attributes related to an entity

NOTE: As defined in ISO/IEC 24760-1:2025 [i.7].

input sanitisation mechanism: function that scans function input data based on a function specific pattern and removes or alters parts, that can lead to incidents

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

NOTE: An input sanitisation mechanism is a security function.

input validation mechanism: function that rejects input data if it does not meet an accepted pattern

EXAMPLE: The input is expected to be the users' year of birth. Data type validation is used to ensure the input to be an integer followed by a range validation checking that the input is between 1900 and the current year.

NOTE: An input validation mechanism is a security function.

integrity protecting communication mechanism: function that protects the integrity of communicated data

NOTE: An integrity protecting communication mechanism is a security function.

integrity protecting secure storage mechanism: function that protects the integrity of persistently stored data

NOTE: An integrity protecting secure storage mechanism is a security function.

logging mechanism: function that ensures storing of audit event data generated by a monitoring mechanism

NOTE: A logging mechanism is a data modification function or a data communication function.

maximal valid derived tokens: maximum number of derived tokens which are considered valid authentication factor at any given time

EXAMPLE 1: $n_{dt,max}$ is 1, where the derived tokens are only generated on demand and invalidated if a new derived token is generated during an other derived tokens T_{VA}.

EXAMPLE 2: $n_{dt,max}$ is $15/1 = 15$ where a derived token is automatically generated every minute and has T_{VA} of 15 minutes.

maximum sustained validation attempt frequency: long term frequency at which an authentication mechanism accepts authentication attempts

EXAMPLE 1: $f_{VA,max}$ is $\frac{5}{5\times 3s+3\,600s} \approx 1{,}4 \times 10^{-3}\,\frac{1}{s}$ for 3 seconds per login attempt + a one-hour waiting period after 5 failed login attempts.

EXAMPLE 2: $f_{VA,max}$ is $\frac{1}{0{,}1s} = 10\,\frac{1}{s}$ for 10 login attempts per second.

EXAMPLE 3: The product $T_{SI} \times f_{VA,max} = 3$, if after three failed attempts, no further attempts can be made.

minimal recommended cryptographic security parameter complexity: number of all possible combinations meeting the minimal recommended number and positions of characters for an authentication mechanisms authentication factor

EXAMPLE 1: $C_{CP,min}$ is 10^5 for a five-digit numerical PIN.

EXAMPLE 2: $C_{CP,min}$ is $9!/(9-5)!$ for an ordered pattern of five non repeating nodes in a 9-node fully connected graph.

EXAMPLE 3: $C_{CP,min}$ is $(26 \times 2 + 10 + 8)^8$ for a password of recommended length of 8 characters from the set of upper and lower case letters, numbers and 8 special characters.

EXAMPLE 4: $C_{CP,min}$ is $2^{2\,048}$ for a 2 048-bit response generated by a security token.

monitoring mechanism: function that (frequently) measures metrics of the SHPSF and generates audit event data

NOTE: A monitoring mechanism is an internal sensing function.

multi factor authentication: authentication method where more than one authentication factor of different types are evaluated by an authentication mechanism

EXAMPLE: Entering a PIN or scanning a Fingerprint in addition to entering an OTP generated by a security token to unlock the front door via the Internet, using a mobile device.

notification mechanism: function that notifies entities on certain events

NOTE: A notification mechanism is a data communication function.

onboarding mechanism: configuration function that is used during the SHPSFs' initialization process

NOTE: A onboarding mechanism is a data modification function that modifies function configuration data.

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

security insurance time: time during which an authentication mechanism is expected to withstand random guessing attacks

NOTE: The T_{SI} is a parameter used to differentiate between authentication strength levels in clause E.1.

single factor authentication: authentication method where only one authentication factor is evaluated by an authentication mechanism

EXAMPLE: Entering a PIN or scanning a Fingerprint to unlock the configuration UI of a SHPSF.

software package verification mechanism: function that verifies the integrity and authenticity of software packages

NOTE: A software package verification mechanism is a security function.

software update mechanism: function that receives and installs software updates

NOTE: A software update mechanism is a data modification function and data communication function where the data are function binary data.

time during which a token is valid: time, after its creation, during which a derived token is accepted as valid by an authentication mechanism

EXAMPLE: An OTP has a time window of maximal 30 minutes after its generation, after which it will no longer be accepted as valid.

3.1.8 Interface

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

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

interface: shared boundary across which the SHPSF exchanges information

logical human interface: interface that is a human interface and a logical interface

EXAMPLE: Web page for remote access.

NOTE: An external client used for remote access providing a logical human interface typically uses a machine interface to communicate with the SHPSF.

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

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

EXAMPLE: Interfaces for USB/Bluetooth®/Ethernet/Wi-Fi®/DECT/DECT-2020 NR or debug ports accessible from outside the SHPSF.

physical human interface: interface that is a human interface and a physical interface

EXAMPLE: Keypad, display, biometric reader, microphone, loudspeaker, (video) camera, touchscreen.

physical interface: interface that is part of the hardware of a SHPSF

EXAMPLE: USB/RJ45/JTAG ports, microSD/SIM card slot.

3.1.9 Operational environments

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.

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

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 wearables.

operational environment: system used to model to likelihood of incidents depending on the physical operational environment of the SHPSF, or parts of it, and the logical operational environment of the relevant logical interfaces.

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.

physical operational environment: operational environment determining the physical accessibility of an architectural component

3.1.10 Use cases

building intercom system: system designed for entry communication in residential or commercial buildings which provides addressing calls, speech and optional video function and is equipped with an electronic unlocking device.

NOTE: This use-case covers, amongst others, building intercom systems as defined in EN IEC 62820 series of standards (IEC 62820-1-1:2026 [i.14], IEC 62820-1-2:2017 [i.15], IEC 62820-2:2017 [i.16], IEC 62820-3-1:2017 [i.17] and IEC 62820-3-2:2018 [i.18]).

fire/gas detection device/system: alarm device or system to detect and notify the presence of a fire or gas hazard into supervised premises

NOTE: This use-case covers, amongst others, smoke alarm devices as defined in EN 14604 [i.19], heat alarm devices as defined in BS 5446-2:2003 [i.20], carbon monoxide alarm devices as defined in EN 50291-1 [i.21] and combustible gases detectors as defined in EN 50194-1 [i.22].

intrusion and hold-up alarm system: alarm system to detect and notify the presence, entry or attempted entry of an intruder into supervised premises and/or alarm system providing the means for a user to deliberately generate a hold-up alarm condition

NOTE: This use-case covers, amongst others, Intrusion and Hold-up Alarm Systems as defined in EN 50131 series of standards (EN 50131-1 [i.23] to EN 50131-13 [i.40]).

social alarm system: alarm system providing 24/7 facilities for alarm triggering, signal transmission, alarm reception, two-way speech communication, reassurance and assistance for people (often older or vulnerable individuals) living independently who may need urgent help

NOTE: This use-case covers, amongst others, Social Alarm Systems as defined in EN 50134 [] series of standards (EN 50134-1 [i.41], EN 50134-2 [i.42], EN 50134-3 [i.43], EN 50134-5 [i.44] and EN 50134-7 [i.45]).

3.1.11 Users

user: natural entity that directly interacts with the SHPSF

NOTE: This includes all natural entities that interact directly with the SHPSF as the final product, but not manufactures for integration in other products.

3.2 Symbols

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

$C_{CP,min}$	Minimal recommended cryptographic security parameter complexity
$f_{VA,max}$	Maximum sustained validation attempt frequency
$L_{CP,eff}$	Effective cryptographic security parameter bitlength
$n_{dt,max}$	Maximal valid derived tokens
p_{GRP}	Cryptographic parameter guessing probability
T_{SI}	Security insurance time
T_{VA}	Time during which a token is valid

3.3 Abbreviations

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

GENERAL

SHPSF	Smart Home Product With Security Functionalities
ACM	Agreed Cryptographic Mechanisms
AES	Advanced Encryption Standard
AES-GCM	Advanced Encryption Standard in Galois/Counter Mode
ARC	Alarm Receiving Centre
BIS	Building Intercom System
CMAC	Cipher-based Message Authentication Code
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DMP	Device Management Platform
DPMP	Device Provisioning and Management Platform
ECC	Elliptic Curve Cryptography
EUF-CMA	Existential Unforgeability under Chosen Message Attack
FAR	False Acceptance Rate
FGS	Fire/Gas Detection Device/System
FRR	False Rejection Rate
GPS	Global Positioning System
GUI	Graphical User Interface
HMAC	Hash-based Message Authentication Code
I&HAS	Intrusion And Hold-Up Alarm System
ICMP	Internet Control Message Protocol
IND-CCA	Indistinguishability under Chosen-Ciphertext Attack
IND-CCA2	Indistinguishability under adaptive Chosen-Ciphertext Attack
IND-CPA	Indistinguishability under Chosen-Plaintext Attack
IP	Internet Protocol
LED	Light Emitting Diode
MFA	Multi Factor Authentication
OTP	One-Time Password
PIN	Personal Identification Number
PitM	Person in the Middle
PSF	residential Physical Security Function
RDPS	Remote Data Processing Solution
ROM	Read Only Memory
RSA	Rivest-Shamir-Adleman
SAS	Social Alarm System
SFA	Single Factor Authentication

SUF-CMA	Strong existential Unforgeability under Chosen Message Attack
TaaS	Telecare as a Service
TLS	Transport Layer Security
UI	User Interface
UPnP	Universal Plug and Play
USB	Universal Serial Bus

COMMUNICATION TYPES

COM	Communication Type
COM.Adjacent	Adjacent Communication
COM.Local	Local Communication
COM.Public	Public Communication
COM.StrictLocal	Strict Local Communication

IMPACT CLASSES

IMP	impact class
IMP.AVAI.LOSS	loss sensitive availability 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	confidentiality 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	function whose use can impact the availability of other devices, services or networks impact class
IMP.FH.DSN.High	function whose use can impact the availability of other devices, services or networks impact class high
IMP.FH.DSN.Low	function whose use can impact the availability of other devices, services or networks impact class low
IMP.FH.DSN.Medium	function whose use can impact the availability of other devices, services or networks impact class medium
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.MINT	function which can modify integrity relevant data impact class
IMP.FH.SP	function whose use can impact the safety or privacy of human entities impact class
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

INTERFACES

IF	interface
IF.Any	unspecified interface
IF.Human	human interface
IF.HumanLogical	logical human interface
IF.HumanPhysical	physical human interface
IF.Logical	logical interface
IF.Machine	machine interface
IF.Physical	physical interface

OPERATIONAL ENVIRONMENTS

LOE	logical operational environment
POE	physical operational environment
POE.Any	unspecified physical operational environment
POE.FullyControlled	fully controlled physical operational environment
POE.Mobile	mobile operational environment
POE.PartiallyControlled	partially controlled physical operational environment

PROTECTION MEASURE STRENGTH LEVEL

AUTH.Basic	authentication - protection strength level basic
AUTH.Enhanced	authentication - protection strength level enhanced
AUTH.Normal	authentication - protection strength level normal
AUTH.Strong	authentication - protection strength level strong
CONF.COM.Basic	communication of confidential data - protection strength level basic
CONF.COM.Enhanced	communication of confidential data - protection strength level enhanced
CONF.COM.Normal	communication of confidential data - protection strength level normal
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.Normal	confidential persistent storage - strength level normal
CONF.SSM.Strong	confidential persistent storage - strength level strong
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.Normal	communication of integrity relevant data - protection strength level normal
INT.SSM.Basic	integrity protecting persistent storage - strength level basic
INT.SSM.Enhanced	integrity protecting persistent storage - strength level enhanced
INT.SSM.Normal	integrity protecting persistent storage - strength level normal
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.Normal	software package integrity verification - strength level normal
N/A	not applicable

4 Product context

4.1 Product functions

4.1.1 Function assets

The present document addresses the following function assets of SHPSF:

- actuator control function
- connection function
- data communication function
- data modification function
- data presenting function
- external sensing function
- fire/gas alarm function
- internal sensing function
- intrusion and hold up alarm function

- other products' configuration function
- physical security notification function
- power supply function
- security function
- SHPSF basic protection object lock function
- SHPSF exterior lock function
- SHPSF high protection object lock function
- SHPSF interior lock function
- SHPSF medium protection object lock function
- social alarm function

NOTE 1: A detailed mapping from the listed function assets to their impact classes is provided in clause D.2.

NOTE 2: Functions in a real SHPSF can fall under several function assets.

4.1.2 Data assets

The function assets might process the following data assets of SHPSF:

- actuator control data
- audit event data
- authorisation policy data
- battery status data
- cryptographic security parameter
- device identifier data
- entity's location data
- fire detection data
- function binary data
- function configuration data
- function fault detection data
- health data
- hold-up detection data
- human emergency detection data
- identity data for authentication
- inflammable/explosive gas detection data
- intrusion detection data
- locking element position data
- logging data

- network status data
- object tamper detection data
- other products' function configuration data
- personal contact data
- personal notes data
- private audio data
- private video data
- public data asset
- real-time data
- SHPSF tamper detection data
- software package
- state data
- window/door opening status data

NOTE 1: A detailed mapping from the listed data assets to their impact classes is provided in clause D.1.

NOTE 2: Data in a real SHPSF can fall under of several data assets.

4.2 Product architecture

The architecture of a SHPSF consists of hardware architectural components and/or software architectural components.

NOTE 1: It is possible that a SHPSF consists of only one hardware architectural component.

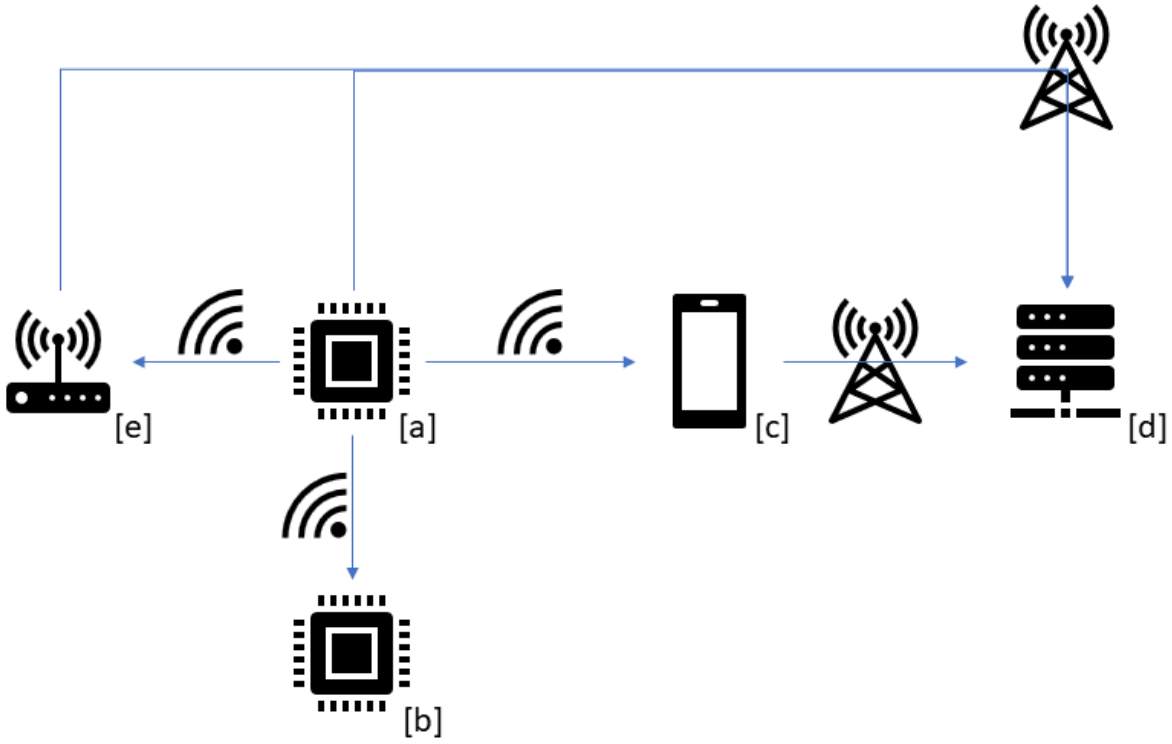

Figure 1: Architectural components and possible connections between them

Exemplary architectural components and possible connections between them are shown in figure 1. The following components are shown in figure 1:

(a) SHPSF's hardware architectural component

(b) Another product's hardware architectural component

(c) SHPSF's mobile application (software architectural component) installed on a smartphone

(d) SHPSF's cloud RDPS (software architectural component) installed on a server

(e) SHPSF's gateway (hardware architectural component)

NOTE 2: Not all subsets of the SHPSF's architectural components in this example are necessary for falling into the scope of the present document.

4.3 Operational environment

4.3.1 General description

Void.

4.3.2 Physical/Hardware environment

The following physical operational environments for:

- any hardware architectural component of the SHPSF; and
- any software architectural component's host device where it is intended or reasonably foreseen to be installed,

are addressed:

- **fully controlled physical operational environment** - POE.FullyControlled;

- **partially controlled physical operational environment** - POE.PartiallyControlled; and
- **mobile operational environment** - POE.Mobile,

by the present document.

4.3.3 Logical/Software environment

For the logical operational environment, the present document addresses the following digital communication types for any architectural component of the SHPSF:

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

4.3.4 Connectivity aspects

The following interfaces, on which physical and digital communication builds upon, are addressed by the present document:

- **human interface** - IF.Human;
- **machine interface** - IF.Machine;
- **logical interface** - IF.Logical; and
- **physical interface** - IF.Physical.

4.4 Distribution of security functions

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

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

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

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

- the SHPSF itself provides those security functions; or
- other products with digital elements in the SHPSF's context provide those security functions.

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

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

4.5 Users

The present document addresses SHPSF having the following using entities:

- Consumers
- Service providers for professional installation, commissioning and/or maintenance
- Manufactures for integration in other products with digital elements intended for consumers

4.6 Use cases

4.6.1 General

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

4.6.2 Specific use cases

In order to support the application of the present document in the context of specific use cases:

- annex H might provide information on the relation of terminology in the context other existing standards to the terminology used in the present document; and
- annex D might provide use case specific refinements on the impact classes associated with data and function assets covered by the present document,

for the following specific use cases:

- SHPSF for BIS;
- SHPSF for FGS;
- SHPSF for I&HAS; and
- SHPSF for SAS.

5 Technical requirements for products

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 its product context.

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.

The application details of some of the technical requirements depend on impact classes for SHPSF functions and data. The impact classes shall be assigned in accordance with

- clause D.1 for data assets; and
- clause D.2 for function assets.

5.2 Appropriate level of cybersecurity

5.2.0 Introduction on appropriate level of cybersecurity requirements

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (1).

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

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

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

Where the SHPSF is intended to be installed or maintained by a consumer for private usage, the SHPSF 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 SHPSF is intended to be installed or maintained by a consumer for private usage, and the SHPSF provides a GUI for security-related configuration function, the SHPSF 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 SHPSF shall support data transfer mechanisms for all loss sensitive data persistently stored at the SHPSF.

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

The SHPSF shall support automatic data transfer mechanisms for all loss sensitive data of impact class [IMP.AVAI.LOSS.Medium] or higher persistently stored at the SHPSF.

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

Where the SHPSF is intended to be installed or maintained by a consumer for private usage, the SHPSF shall support data export mechanisms for all loss sensitive data of impact class [IMP.AVAI.LOSS.Medium] or higher persistently stored at the SHPSF 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 Introduction on no known exploitable vulnerabilities

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (a).

5.3.1 [NKEV-MKAV] No known exploitable vulnerabilities

The SHPSF 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 SHPSF.

NOTE 1: The known exploitable vulnerabilities that occur after making the SHPSF available on the market are subject to the vulnerability handling in prEN 40000-1-3 [i.5].

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

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

The SHPSF's architectural components shall:

- request information on the availability of security update packages; and
- notify users when security update packages are available; and
- (if not blocked by the entity that puts the architectural component into first use) request and install available security update packages,

before or during first use.

5.4 Secure by default configuration

5.4.0 Introduction on secure by default configuration

This clause addresses the requirements in the Regulation (EU) 2024/2847 [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 SHPSF 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 2,

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 SHPSF 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; and

- automatic installation of updates does not create an unacceptable risk to essential function availability or safety,

each 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 [SU-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.

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

The SHPSF shall by default be configured to use automated notification of its users, when updates of the SHPSF's software are available.

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

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

All hardware architectural components of the SHPSF shall provide a factory reset mechanism that allows a user to restore the default state, including the secure deletion of all user-related data, installed applications, and configurations deviating from the default state.

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 SHPSF are informed about secure decommissioning of the SHPSF.

5.4.5 [SDC-MON-HANDLE] Handling of events by default

The SHPSF shall by default be configured to use:

- a logging mechanism; or
- where the architectural component does not support public communication, a data transfer mechanism,

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

5.4.6 [CRY-GENERAL] General requirements related to cryptography

The SHPSF shall comply with the technical requirements provided in annex K.

5.4.7 [CRY-CCK-PRE-LEN] Key size of preinstalled long term confidential cryptographic keys

The SHPSF shall only provide preinstalled long term confidential cryptographic keys of key sizes that are:

- listed in Agreed Cryptographic Mechanisms [1]; or
- provide a minimum security strength of 112 bit.

5.4.8 [CRY-CCK-GEN] Default key size of generated long term confidential cryptographic keys

The SHPSF shall by default only generate long term confidential cryptographic keys of key sizes that are:

- listed in Agreed Cryptographic Mechanisms [1]; or

- provide a minimum security strength of 112 bit.

5.4.9 [CRY-PW-PRE-COM] Complexity of preinstalled passwords

The SHPSF shall only provide preinstalled passwords:

- that meet the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) determined by the corresponding authentication mechanisms' usage according to table 2 and corresponding assessments; and
- that are either:
  - individual per SHPSF and not derivable via publicly available information; or
  - random per SHPSF.

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

The SHPSF shall by default only generate passwords:

- that meet the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) determined by the corresponding authentication mechanisms' usage according to table 2 and corresponding assessments; and
- that are random.

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

The SHPSF shall only use user chosen passwords that meet the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) determined by the corresponding authentication mechanisms' usage according to table 2 and corresponding assessments, except for user chosen passwords where the user explicitly confirms their usage after a warning by the SHPSF.

5.5 Security updates

5.5.0 Introduction on security updates

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (c).

5.5.1 [SU-SUPPORT] Secure software update mechanism

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

NOTE 1: A mobile application, as part of a SHPSF, can be developed and distributed, such that it will receive security updates via the software update mechanism of the host system's application distribution platform. Thus, the SHPSF supports a software update mechanism for the mobile application.

NOTE 2: A device, as part of a SHPSF, can be developed such that its entire software can be updated via its core software's software update mechanism. Thus, the device supports a software update mechanism for its software. In this case the software update mechanism is provided by the core software of the device.

NOTE 3: Part of the SHPSF's software can be immutable due to the technology which is used to store its executable code (e.g. software installed in a ROM).

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

All architectural components of the SHPSF that include core software shall provide software update mechanisms, that allow security updates for every part of the architectural component's software, except for parts of the architectural components software, that are immutable due to security.

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

5.5.3 [SU-AUTO] Automated security updates

Where:

- the SHPSF 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 SHPSF 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 egress during a fire alarm, preventing prompt access for emergency responders, or preventing timely arming/disarming/panic activation during an intrusion event).

NOTE 2: Where automated security updates are not supported, the user will typically be informed (e.g. via the SHPSF'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 SHPSF provides mechanisms for automated security update of SHPSF's software operated by users, the SHPSF 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 SHPSF provides mechanisms for automated security update of SHPSF's software operated by users, the SHPSF shall provide an option for users to temporarily postpone the automated installation of updates.

NOTE: The time to postpone the automated installation of security updates can be set by the user.

5.5.6 [SU-NOTIF] Update notifications

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

5.6 Authentication and access control

5.6.0 Introduction on authentication and access control

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (d).

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

The SHPSF 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 1 except for connection functions.

Table 1: Assignment for access control mechanisms

<table>
<tr><td colspan="3"></td><td colspan="3">Impact class for function whose use can cause harm</td></tr>
<tr><td colspan="3"></td><td>IMP.FH.Low</td><td>IMP.FH.Medium</td><td>IMP.FH.High</td></tr>
<tr><td rowspan="9">Attack Surface determined by COM, IF and POE of the architectural component that receives function trigger input</td><td rowspan="3">COM.StrictLocal via IF.Any</td><td>POE.FullyControlled</td><td>N/A</td><td>N/A</td><td>applicable[*]</td></tr>
<tr><td>POE.PartiallyControlled</td><td>N/A</td><td>applicable</td><td>applicable</td></tr>
<tr><td>POE.Mobile</td><td>applicable</td><td>applicable</td><td>applicable</td></tr>
<tr><td rowspan="3">COM.Local via IF.HumanPhysical</td><td>POE.FullyControlled</td><td>N/A</td><td>applicable</td><td>applicable</td></tr>
<tr><td>POE.PartiallyControlled</td><td>applicable</td><td>applicable</td><td>applicable</td></tr>
<tr><td>POE.Mobile</td><td>applicable</td><td>applicable</td><td>applicable</td></tr>
<tr><td>COM.Local via a non-IF.HumanPhysical</td><td rowspan="3">POE.Any</td><td>applicable</td><td>applicable</td><td>applicable</td></tr>
<tr><td>COM.Adjacent via IF.Any</td><td>applicable</td><td>applicable</td><td>applicable</td></tr>
<tr><td>COM.Public via IF.Any</td><td>applicable</td><td>applicable</td><td>applicable</td></tr>
<tr><td colspan="6">For protection measures that are labelled with [*] it is not required that the SHPSF uses access control mechanisms for its following functions:
- factory reset function</td></tr>
</table>

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

Where the authorisation policy restricts permissions, the SHPSF 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 2,

except for connection functions.

Table 2: Assignment for authentication mechanisms strengths

			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 the architectural component that receives function trigger input	COM.StrictLocal via IF.Any	POE.FullyControlled	N/A	N/A	AUTH.Normal[*]
		POE.PartiallyControlled	N/A	AUTH.Basic	AUTH.Normal
		POE.Mobile	AUTH.Basic	AUTH.Normal	AUTH.Enhanced
	COM.Local via IF.HumanPhysical	POE.FullyControlled	N/A	AUTH.Basic	AUTH.Normal
		POE.PartiallyControlled	AUTH.Basic	AUTH.Normal	AUTH.Enhanced
		POE.Mobile	AUTH.Basic	AUTH.Normal	AUTH.Enhanced
	COM.Local via a non-IF.HumanPhysical	POE.Any	AUTH.Normal	AUTH.Normal	AUTH.Enhanced
	COM.Adjacent via IF.Any		AUTH.Normal	AUTH.Normal	AUTH.Enhanced
	COM.Public via IF.Any		AUTH.Normal	AUTH.Enhanced	AUTH.Enhanced
For protection measures that are labelled with [*] it is not required that the SHPSF uses authentication mechanisms for its following functions: - factory reset function					

5.6.3 [AUTHZ-LP] Least privilege in authorisation policies

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

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

5.6.4 [AUTHZ-R] Revocability of granted permissions

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

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

5.7 Confidentiality protection

5.7.0 Introduction on confidentiality protection

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (e).

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

The SHPSF shall use confidentiality protecting secure storage mechanisms for persistently stored confidential data, where the mechanisms' strength are specified in clause E.3.1 and the minimal required mechanisms' strength are determined by table 3.

NOTE: 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 3: 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 the architectural component that persistently stores confidential data	POE.FullyControlled	N/A	N/A	N/A
	POE.PartiallyControlled	N/A	CONF.SSM.Basic[*]	CONF.SSM.Normal
	POE.Mobile	CONF.SSM.Basic[*]	CONF.SSM.Normal	CONF.SSM.Enhanced
For protection measures labelled with [*], it is not required that the SHPSF 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 SHPSF 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.3.3 and the minimal required confidentiality protection measures' strength are determined by table 4.

NOTE: The SHPSF can communicate data with other devices or services and between architectural components, e.g. between a SHPSF's hardware architectural component and its RDPS.

Table 4: 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 the architectural component that communicates confidential data	COM.Local via IF.Machine or IF.HumanLogical	POE.FullyControlled	N/A	N/A	CONF.COM.Normal[*]
		POE.PartiallyControlled	N/A	CONF.COM.Basic[*]	CONF.COM.Normal[*]
		POE.Mobile	CONF.COM.Basic[*]	CONF.COM.Normal[*]	CONF.COM.Enhanced[*]
	COM.Adjacent via IF.Any	POE.Any	CONF.COM.Enhanced[*]	CONF.COM.Enhanced[*]	CONF.COM.Enhanced[*]
	COM.Public via IF.Any		CONF.COM.Enhanced[*]	CONF.COM.Enhanced[*]	CONF.COM.Enhanced[*]
For protection measures labelled with [*], it is not required that the SHPSF uses confidentiality protecting communication mechanisms for confidential data: - which is used as connection data.					

5.8 Integrity protection

5.8.0 Introduction on integrity protection

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (f).

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

The SHPSF shall use integrity protecting secure storage mechanisms for persistently stored integrity relevant data, where the mechanisms' strength are specified in clause E.2.1 and the minimal required mechanisms strength are determined by table 5.

Table 5: 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.Normal
	POE.Mobile	INT.SSM.Basic[*]	INT.SSM.Normal	INT.SSM.Enhanced
For protection measures labelled with [*], it is not required that the SHPSF uses integrity protecting persistent storage for integrity relevant data: - which is persistently stored on non-removable storage.				

5.8.2 [INT-COM] Communication of integrity relevant data

The SHPSF 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.

NOTE: The SHPSF can communicate data with other devices or services and between architectural components, e.g. between a SHPSF's hardware architectural component and its RDPS.

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 the architectural component that communicates integrity relevant data	COM.StrictLocal via IF.Machine	POE.Any	INT.COM.Basic	INT.COM.Basic	INT.COM.Basic
	COM.Local via IF.Machine or IF.HumanLogical	POE.FullyControlled	INT.COM.Basic	INT.COM.Basic	INT.COM.Normal[*]
		POE.PartiallyControlled	INT.COM.Basic	INT.COM.Normal[*]	INT.COM.Enhanced[*]
		POE.Mobile	INT.COM.Basic	INT.COM.Normal[*]	INT.COM.Enhanced[*]
	COM.Adjacent via IF.Any	POE.Any	INT.COM.Enhanced[*]	INT.COM.Enhanced[*]	INT.COM.Enhanced[*]
	COM.Public via IF.Any		INT.COM.Enhanced[*]	INT.COM.Enhanced[*]	INT.COM.Enhanced[*]
For protection measures labelled with [*], it is not required that the SHPSF 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.					

5.8.3 [INT-SWPCK] Software package verification

The SHPSF 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.2.5 and where the minimal software package verification mechanism's strength is determined by table 7.

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

Table 7: 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 the architectural component over which the software package is received	COM.StrictLocal	INT.SW.VER.Basic	INT.SW.VER.Basic	INT.SW.VER.Basic
	COM.Local, COM.Adjacent or COM.Public	INT.SW.VER.Normal	INT.SW.VER.Normal	INT.SW.VER.Enhanced

5.9 Data minimisation

5.9.0 Introduction on data minimisation

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (g).

5.9.1 [DMIN-DJST] Minimise processed data

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

EXAMPLE: The SHPSF provides documentation that specifies the conditions under which audio or video 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 Introduction on availability protection

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (h).

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

A hardware architectural component 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 SHPSF shall ensure that local operability of this function is supported in case of a loss of network access.

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

The SHPSF shall use a mechanism to attempt to reconnect cleanly after a loss of network connection.

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

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.

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 SHPSF, the SHPSF shall use a mechanism to warn the user before or at least during a 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 a hardware architectural component and sends a notification to the user.

NOTE: A mechanism to warn the user cannot ensure that the user receives the warning. For example, a SHPSF with only local communication connectivity placed in a summer house may run out of battery before the user warning is delivered. However, the user would have been warned when being present before battery exhaustion.

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 SHPSF, the SHPSF shall use a mechanism to notify the user before the hardware architectural component restrains the use of power when the SHPSF recognizes low power condition.

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

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

5.10.6 [AVAI-TIME-NET-PRIO] Network prioritization

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 SHPSF, the SHPSF shall use a mechanism to prioritize its use of network resources in case of a network resource conflict:

- such that these functions are prioritized according to their time sensitive availability impact class (IMP.AVAI.TIME); or
- such that functions are prioritized according to user decisions or configuration.

5.10.7 [AVAI-TIME-RES-PRIO] Power resource prioritization

Where:

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

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

- such that these functions are prioritized according to their time sensitive availability impact class (IMP.AVAI.TIME); or
- such that functions are prioritized according to user decisions or configuration.

5.10.8 [AVAI-TIME-DOS-RATE] Incoming rate limiting

Where at least one time sensitive function with IMP.AVAI.TIME.High AND at least one machine interface are provided by the SHPSF, the SHPSF shall use mechanisms to discard packets from a source if it sends an unusually high number of requests, whose execution could result in a resource conflict.

5.10.9 [AVAI-SUM-SCHEDULE] Scheduling of updates

Where:

- the SHPSF 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 an architectural component,

the SHPSF shall support the scheduling of the application of updates of those architectural components.

5.11 Non-interference

5.11.0 Introduction on non-interference

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (i).

5.11.1 [NOINF-AMP] Amplification control

Where at least one function whose use can impact the availability of other devices, services or networks with IMP.FH.DSN.Medium or higher is provided by the SHPSF, the SHPSF shall use mechanisms to prevent effective amplification of requests or network traffic of these functions.

EXAMPLE: An ICMP request has an amplification factor of three. Then the response time is artificially extended by a factor of three per destination to have no effective gain in bandwidth.

5.12 Attack surface minimisation

5.12.0 Introduction on attack surface minimisation

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (j).

5.12.1 [LAS-INVAL] Validation of external data input

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

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

EXAMPLE: If an application expects the input to be an email address, any input that does not conform to the format of an e-mail address will be rejected.

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.

5.12.2 [LAS-INSAN] Sanitisation of external data input

The SHPSF shall use input sanitisation mechanisms at 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 (defined by a corresponding function specific pattern) 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

hardware architectural components shall only provide physical interfaces, that are necessary for the SHPSF's intended purpose.

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

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

5.12.5 [LAS-APP] Only necessary apps by default

The SHPSF shall by default only provide installed application software, that are necessary for its intended purpose.

5.12.6 [LAS-SBOOT] Secure boot

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

NOTE 1: The requirement corresponds to the verified boot capability in ETSI EN 304 623 (V1.1.1) [i.6].

NOTE 2: The SHPSF 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 Introduction on exploit mitigation

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (k).

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

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

- time sensitive function with [IMP.AVAI.TIME.High]; and
- 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 SHPSF's intended purpose.

5.14 Monitoring

5.14.0 Introduction on monitoring

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (l).

5.14.1 [MON-LOW] Events to log for low risk SHPSF

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

- change of configuration affecting core software;
- starts, shutdowns or other changes of operational states of core software;
- errors of the core software.

5.14.2 [MON-MEDIUM] Events to log for medium risk SHPSF

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

- unsuccessful authentication attempt;
- change of configuration affecting core software;
- starts, shutdowns or other changes of operational states of core software;
- errors of the core software;
- unsuccessful attempt of an identity to gain additional privileges;
- unsuccessful attempt of an identity to access a data asset or function asset.

5.14.3 [MON-HIGH] Events to log for high risk SHPSF

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

- every authentication attempt;
- change of configuration affecting core software;
- starts, shutdowns or other changes of operational states of core software;
- change of configuration affecting application software that realize functions whose use can cause harm of impact class high;
- starts, shutdowns or other changes of operational states of application software who realize function whose use can cause harm of impact class high;
- errors of the core software;
- errors of the application software who realize function whose use can cause harm of impact class high;
- every attempt of an identity to gain additional privileges;
- every attempt of an identity to access a data asset or function asset.

5.14.4 [MON-HANDLE] Handling of events

The SHPSF shall support:

- a logging mechanism; or
- where the architectural component does not support public communication, 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 SHPSF does not have a function whose use can cause harm of impact class high, the SHPSF shall use at least a time service or function to include a timestamp in every audit event data, permanently stored by the SHPSF.

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

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

5.14.7 [LOG-STORE-MEDIUM] Logfile persistence for medium risk SHPSF

Where the SHPSF has a function whose use can cause harm of impact class medium as its highest function impact class, the SHPSF 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 SHPSF

Where the SHPSF has a function whose use can cause harm of impact class high as its highest function impact class, the SHPSF 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 SHPSF uses logging mechanisms the SHPSF shall provide a clear and easy to use option for users to disable those mechanisms.

5.15 Factory reset and data portability

5.15.0 Introduction on factory reset and data portability

This clause addresses the requirements in the Regulation (EU) 2024/2847 [i.1] Annex I Part I (2) (m).

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

The SHPSF 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 General

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.

In order to assess the compliance with the requirements listed in clause 5 of the present document, the assessment procedures described in clause 6 are to be followed. When performing assessments, the distribution of security functions (see clause 4.4) are to be considered, including whether the product provides security functions itself, demands them from other products with digital elements within its context, or supplies them to other products with digital elements.

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

- are covering the same assessment activities as described in clause 6, and
- are valid for the moment of the assessment to be performed under clause 6,

those existing evidences can be used for the "assessment verdict" and as "assessment evidence".

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 unauthorised 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 include, 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 reference:

[USERNOT-NOSECFUC]

Assessment objective:

The assessment covers:

- a conceptual assessment of [USERNOT-NOSECFUC].

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a list of SHPSF's architectural components; and
- 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; and
  - 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; and
  - a description of the mechanisms to detect and notify the user when those functions are not available.

Assessment activities:

- The SHPSF'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 SHPSF's conformity to [USERNOT-NOSECFUC].

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 reference:

[USERNOT-SECREL]

Assessment objective:

The assessment covers:

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

Assessment preparation:

The following documentation for the SHPSF 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 SHPSF'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 SHPSF'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.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the SHPSF'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 reference:

[GUI-SECCONF]

Assessment objective:

The assessment covers:

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

Assessment preparation:

The following documentation for the SHPSF 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 SHPSF's GUI for security-related configuration function.

Assessment activities:

- The SHPSF's conformity to [GUI-SECCONF] shall be validated based on the documentation.
- The correctness of the implementation shall be verified by inspecting for each SHPSF'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 is 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 SHPSF'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 reference:

[BACKUP-TRANS]

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a list of SHPSF's architectural components; and
- for each architectural component:
  - a list of loss sensitive data persistently stored at the architectural component; and
  - 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 SHPSF 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 SHPSF'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 SHPSF's physical human interfaces for persistently stored loss sensitive data; and
  - a scan of the SHPSF'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 SHPSF'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 reference:

[BACKUP-AUTOTRANS]

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a list of SHPSF's architectural components; and
- 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; and
  - 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 SHPSF 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 SHPSF'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 SHPSF's physical human interfaces for persistently stored loss sensitive data of impact class [IMP.AVAI.LOSS.Medium] or higher; and
  - a scan of the SHPSF'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 SHPSF'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 reference:

[BACKUP-EXPORT]

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a list of SHPSF's architectural components; and
- 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; and

- 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 SHPSF 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 SHPSF'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 SHPSF's physical human interfaces for persistently stored loss sensitive data of impact class [IMP.AVAI.LOSS.Medium] or higher; and
  - a scan of the SHPSF'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 SHPSF'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 reference:

[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 SHPSF required by clause 5.4; and
- (if the assessment is based on a vulnerability scanner) a functional completeness assessment of the identified known exploitable vulnerabilities beneath the documented remediation plan.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

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

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

- the SHPSF shall be set up in default configuration; and
- a vulnerability scanner for the SHPSF shall be set up.

Assessment activities:

- A list of potential vulnerabilities shall be created either by:
  - (if the assessment is based on an SBOM and the SBOM is transitive) consulting https://euvd.enisa.europa.eu/ based on the SHPSF's details including the transitive SBOM and analysing the results for known exploitable vulnerabilities; or
  - (if the assessment is based on a vulnerability scanner) applying the vulnerability scanner on the SHPSF and analysing the results for known exploitable vulnerabilities.
- The SHPSF'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-UDP]

Assessment reference:

[NKEV-INIT-UDP]

Assessment objective:

The assessment covers:

- a conceptual assessment of [NKEV-INIT-UDP]; and
- a functional sufficiency assessment the SHPSF´s behaviour on first start or after factory reset to fulfil [NKEV-INIT-UDP],

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF 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; and
    - interfaces and network connections used by the software update mechanisms; and
    - notification mechanisms to notify users when security update packages are available; and
    - interfaces and network connections used by the software update mechanisms.

The following test setups shall be prepared:

- SHPSF in its default configuration; and
- documented interfaces and network connections used by software update mechanisms or notification mechanisms.

Assessment activities:

- The SHPSF's conformity to [NKEV-INIT-UDP] 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; and
  - verify whether users are notified when security update packages are available; and
  - 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 SHPSF's conformity with [NKEV-INIT-UDP]; 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 reference:

[SDC-AUM-FH]

Assessment objective:

The assessment covers:

- a conceptual assessment of [SDC-AUM-FH]; and
- a functional completeness assessment on the SHPSF'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 SHPSF to fulfil [SDC-AUM-FH] is addressed by the assessment of [AUM-FH].

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a list of SHPSF's functions whose use can cause harm that are enabled in the factory default state or can be activated during initialization; and
- for each of those functions:
  - the physical operational environment of the architectural component that performs the function; and
  - for each of the function's trigger input possibilities:
    - the interface and communication type; and
    - 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 SHPSF in factory default state and after initialization.

Assessment activities:

- The SHPSF'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 SHPSF in factory default state; and

- (if functions whose use can cause harm can be configured during initialization) performing the initialization without providing explicit confirmation of configurations deviating from the minimal required authentication strength determined by table 2 and inspecting the SHPSF after initialization.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the SHPSF'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 reference:

[SDC-SUM-AUTO]

Assessment objective:

The assessment covers:

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

based on the factory default state.

Assessment preparation:

The following documentation for the SHPSF'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 initialization; and
- documentation describing updatable parts of the SHPSF's software were automated security updates are not used in the factory default state or activation is not supported during initialization; and
- (if the SHPSF does not use automated security updates in the factory default state or activation of use is not supported during initialization for an updatable part of its software):
  - a justified statement that each of the SHPSF's architectural component has no capability to connect to public networks; or
  - for each updatable part of the SHPSF's software that does not use automated security updates in the factory default state or activation is not supported during initialization 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 initialization:
  - a test setup that allows to perform a corresponding automated security update.

Assessment activities:

- The SHPSF'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 initialization, its correct implementation shall be verified by:
  - initializing the SHPSF without changes to the preconfigured settings; and
  - providing a corresponding software package in a form that triggers the automated security update; and
  - checking whether the SHPSF 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 SHPSF'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 initialization

6.4.3 Assessment criteria for [SDC-SUM-NOTIF]

Assessment reference:

[SDC-SUM-NOTIF]

Assessment objective:

The assessment covers:

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

based on the factory default state.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- documentation describing all supported software update notification mechanisms where software update notification are used in the factory default state or whose use can be activated during initialization, including:
  - a description of how software update notifications are triggered; and
  - a description of how notifications are received; and

- documentation describing parts of the SHPSF's updatable software where software update notification is not used in the factory default state or whose use cannot be activated during initialization, including:
  - (if the SHPSF does not use software update notification in the factory default state or whose use cannot be activated during initialization for an updatable part of its software), a justified statement that each of the SHPSF'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 initialization:
  - 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 SHPSF in default configuration.

Assessment activities:

- The SHPSF'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 initialization, its correct implementation shall be verified by:
  - initializing the SHPSF without changes to the preconfigured settings; and
  - triggering a software update notification; and
  - checking whether the software update notification mechanism automatically notifies the SHPSF's users.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the SHPSF'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 initialization 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 initialization was successful

6.4.4 Assessment criteria for [SDC-FRM]

Assessment reference:

[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:

The following documentation for the SHPSF shall be complete:

- documentation on how the factory reset mechanism can be accessed; and
- the SHPSF shall be set up and some configuration changes shall be created and persistently stored; and
- where the SHPSF supports the storage of user-related data, some user-related data shall be created and persistently stored on the SHPSF; and
- where the SHPSF supports the installation of applications, some common application for the SHPSF 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-MON-HANDLE]

Assessment reference:

[SDC-MON-HANDLE]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of each audit event data generated by a monitoring mechanism of the SHPSF 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 SHPSF shall be complete:

- for each architectural component:
  - documentation on support of public communication; and

- 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; and
  - access the storage location where logging data is stored; and
- for each data transfer mechanism in *assessment preparation*, a test setup that allows to:
  - generate audit event data; and
  - 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; and
- 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 SHPSF's conformity with [SDC-MON-HANDLE]; and
- 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

6.4.6 Assessment criteria for [CRY-GENERAL]

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

6.4.7 Assessment criteria for [CRY-CCK-PRE-LEN]

Assessment reference:

[CRY-CCK-PRE-LEN]

Assessment objective:

The assessment covers:

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

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a list of SHPSF's preinstalled long term confidential cryptographic keys; and
- for each preinstalled long term confidential cryptographic key:
  - a description of generation method of the confidential cryptographic key; and
  - its key sizes and corresponding security strength including a justification for the security strength.

The following test setups shall be prepared:

- for each architectural component, a test setup for identifying and analysing preinstalled long term confidential cryptographic keys.

Assessment activities:

- The SHPSF'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 SHPSF'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

6.4.8 Assessment criteria for [CRY-CCK-GEN]

Assessment reference:

[CRY-CCK-GEN]

Assessment objective:

The assessment covers:

- a conceptual assessment of [CRY-CCK-GEN]; and

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

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a list of SHPSF's long term confidential cryptographic key generation mechanisms; and
- for each long term confidential cryptographic key generation mechanism:
  - a description of the confidential cryptographic key generation mechanism; and
  - 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 SHPSF'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 SHPSF in default configuration.

Assessment activities:

- The SHPSF's conformity to [CRY-CCK-GEN] shall be validated based on the documentation.
- For each SHPSF'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 SHPSF's conformity to [CRY-CCK-GEN]; and
- the verification of the correct implementation of each SHPSF'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 SHPSF's long term confidential cryptographic key generation mechanism

6.4.9 Assessment criteria for [CRY-PW-PRE-COM]

Assessment reference:

[CRY-PW-PRE-COM]

Assessment objective:

The assessment covers:

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

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a list of SHPSF's preinstalled passwords; and
- for each preinstalled password:
  - a description of generation method of the password; and
  - 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.

The following test setups shall be prepared:

- for each architectural component, a test setup for identifying and analysing preinstalled passwords.

Assessment activities:

- The SHPSF'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 SHPSF'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

6.4.10 Assessment criteria for [CRY-PW-GEN-COM]

Assessment reference:

[CRY-PW-GEN-COM]

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a list of SHPSF's password generation mechanisms; and

- for each password generation mechanism:
  - a description of the password generation mechanism; and
  - a list of generated passwords; and
  - 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 SHPSF's password generation mechanism, a test setup for generating and extracting corresponding passwords based on a sample SHPSF in default configuration.

Assessment activities:

- The SHPSF's conformity to [CRY-PW-GEN-COM] shall be validated based on the documentation.
- For each SHPSF'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 SHPSF's conformity to [CRY-PW-GEN-COM]; and
- the verification of the correct implementation of each SHPSF'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 SHPSF's password generation mechanism

6.4.11 Assessment criteria for [CRY-PW-USR-COM]

Assessment reference:

[CRY-PW-USR-COM]

Assessment objective:

The assessment covers:

- a conceptual assessment of [CRY-PW-USR-COM]; and
- a functional completeness assessment of each option for users to choose passwords; and
- 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 SHPSF shall be complete:

- a list of SHPSF's options for users to choose passwords; and

- 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; and
  - a statement whether users can choose passwords deviating from the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$); and
  - (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 SHPSF in default configuration; and
- for each architectural component, a test setup for identifying and analysing options for users to choose passwords.

Assessment activities:

- The SHPSF'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 SHPSF'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 reference:

[SU-SUPPORT]

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a list of all architectural components of the SHPSF; and
- for each architectural component:
  - a list of its software including a declaration of immutability; and
  - for each software that are declared immutable, a technical description on the corresponding measures including a justification for the immutable design; and
  - 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 SHPSF in default configuration; and
- for each software update mechanism, a test setup that allows to perform an update over that software update mechanism.

Assessment activities:

- The SHPSF'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 SHPSF 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 SHPSF'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 reference:

[SU-PROVIDE]

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a list of all architectural components of the SHPSF that include core software; and
- a list of architectural components declared immutable, including technical justification; and
- 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 SHPSF in default configuration; and
- for each software update mechanism, a test setup that allows to perform an update over that software update mechanism.

Assessment activities:

- The SHPSF'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 SHPSF 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 SHPSF'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 reference:

[SU-AUTO]

Assessment objective:

The assessment covers:

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

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

Assessment preparation:

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

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

- documentation describing updatable parts of the SHPSF's software that do not support automated security updates; and
- (if the SHPSF does not support automated security updates for an updatable part of its software):
  - a justified statement that each of the SHPSF's architectural component has no capability to connect to public networks; or
  - for each updatable part of the SHPSF'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 SHPSF'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; and
  - 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 SHPSF'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 reference:

[SU-DISABLE-AUTO]

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

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

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 SHPSF'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 disable mechanisms implementation shall be verified by:
  - disabling the software update mechanism as documented; and
  - providing a corresponding software package in a form that triggers the automated security update; and
  - checking that the product does not perform the automated security update.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the SHPSF'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 reference:

[SU-POSTPONE-AUTO]

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- list of all software update mechanism that support automated security updates; and
- documentation on how to postpone automated updates; and
- documentation on entities intended to operate the SHPSF.

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 SHPSF'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; and
  - providing a corresponding software package in a form that triggers the automated security update; and
  - 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 SHPSF's conformity with [SU-POSTPONE-AUTO]; and
- the verification of the correct implementation of the mechanism to temporarily 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 temporarily postpone the automated installation of updates

6.5.6 Assessment criteria for [SU-NOTIF]

Assessment reference:

[SU-NOTIF]

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF 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 SHPSF's updatable software where software update notification is not supported; and
- (if the SHPSF does not support software update notification for an updatable part of its software):
  - a justified statement that each of the SHPSF'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 SHPSF in default configuration.

Assessment activities:

- The SHPSF'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 SHPSF's users that an update of its software is available.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the SHPSF'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 reference:

[ACM-FH]

Assessment objective:

The assessment covers:

- a conceptual assessment of [ACM-FH]; and
- a functional completeness assessment on the SHPSF capabilities that are addressed by [ACM-FH]; and
- a functional sufficiency assessment of each access control mechanism used by the SHPSF to fulfil [ACM-FH],

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a list of SHPSF's functions whose use can cause harm; and
- for each function whose use can cause harm:
  - its impact class IMP.FH; and
  - the physical operational environment of the architectural component that performs the function; and
  - for each of the function's trigger input possibilities:
    - the interface and communication type; and
    - 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 SHPSF in default configuration; and
- for each access control mechanism, a test setup that allows privilege escalation attacks from authenticated entities and unauthorised access attempts of unauthenticated entities.

Assessment activities:

- The SHPSF'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 SHPSF for functions and related access control mechanisms that are accessible via physical human interfaces; and
  - a scan of the SHPSF 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; and
  - unauthorised 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 SHPSF'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 reference:

[AUM-FH]

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a list of SHPSF'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 SHPSF 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 SHPSF'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 SHPSF for functions and related authentication mechanisms that are accessible via physical human interfaces;
  - a scan of the SHPSF 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 SHPSF'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 reference:

[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 SHPSF 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 SHPSF'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 SHPSF'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 reference:

[AUTHZ-R]

Assessment objective:

The assessment covers:

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

Assessment preparation:

The following documentation for the SHPSF 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; and
  - 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]

6.7 Confidentiality protection

6.7.1 Assessment criteria for [CONF-SSM]

Assessment reference:

[CONF-SSM]

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a list of SHPSF's confidential data that are intended to be persistently stored by the SHPSF; and
- for each confidential data that are intended to be persistently stored by the SHPSF:
  - its impact class IMP.CONF; and
  - a list of architectural components that store the confidential data including:
    - its physical operational environment; and
    - a list of storage locations for the confidential data; and
    - 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 SHPSF in default configuration; and
- 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 SHPSF'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 SHPSF's physical human interfaces for persistently storable/stored confidential data, related storage locations and confidentiality protecting secure storage mechanisms; and
  - a scan of the SHPSF'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 SHPSF'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 reference:

[CONF-COM]

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a list of SHPSF's confidential data that are intended to be communicated by or to the SHPSF; and
- for each confidential data that are intended to be communicated by or to the SHPSF:
  - its impact class IMP.CONF; and
  - a list of architectural components that can communicate the confidential data including:
    - its physical operational environment; and
    - the corresponding interfaces and communication types; and
    - 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 SHPSF in default configuration for identifying:
  - confidential data that can be communicated by or to the architectural component; and
  - the corresponding interfaces and communication types for communication; and
  - the corresponding confidentiality protecting communication mechanisms; and
- 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 SHPSF'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 SHPSF's physical human interfaces for communicable confidential data, related communication capabilities and confidentiality protecting communication mechanisms; and
  - a scan of the SHPSF'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 SHPSF'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

6.8 Integrity protection

6.8.1 Assessment criteria for [INT-SSM]

Assessment reference:

[INT-SSM]

Assessment objective:

The assessment covers:

- a conceptual assessment of [INT-SSM]; and

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

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a list of SHPSF's integrity relevant data that are intended to be persistently stored by the SHPSF; and
- for each integrity relevant data that are intended to be persistently stored by the SHPSF:
  - its impact class IMP.INT; and
  - a list of architectural components that store the integrity relevant data including:
    - its physical operational environment; and
    - a list of storage locations for the integrity relevant data; and
    - 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 SHPSF in default configuration; and
- 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 SHPSF'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 SHPSF's physical human interfaces for persistently storable/stored integrity relevant data, related storage locations and integrity protecting secure storage mechanisms; and
  - a scan of the SHPSF'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 SHPSF'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-COM]

Assessment reference:

[INT-COM]

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a list of SHPSF's integrity relevant data that are intended to be communicated by or to the SHPSF; and
- for each integrity relevant data that are intended to be communicated by or to the SHPSF:
  - its impact class IMP.CONF; and
  - a list of architectural components that can communicate the integrity relevant data including:
    - its physical operational environment; and
    - the corresponding interfaces and communication types; and
    - 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 SHPSF in default configuration for identifying:
  - integrity relevant data that can be communicated by or to the architectural component; and
  - the corresponding interfaces and communication types for communication; and
  - the corresponding integrity protecting communication mechanisms; and
- 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 SHPSF'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 SHPSF's physical human interfaces for communicable integrity relevant data, related communication capabilities and integrity protecting communication mechanisms; and

  - a scan of the SHPSF'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 SHPSF'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

6.8.3 Assessment criteria for [INT-SWPCK]

Assessment reference:

[INT-SWPCK]

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a list of the SHPSF's architectural components; and
- for each architectural component:
  - a list of mechanisms to install software packages; and
  - for each SHPSF's mechanism to install software packages:
    - the communication types of over which software packages can be received; and
    - a list of software that can be installed by the mechanism including the maximum impact class IMP.INT of corresponding software packages; and
    - 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 SHPSF in default configuration; and
- 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 SHPSF'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 SHPSF's physical human interfaces for mechanism to install software packages; and
  - a scan of the SHPSF's logical interfaces for mechanism to install software packages; and
  - 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 SHPSF'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

6.9 Data minimisation

6.9.1 Assessment criteria for [DMIN-DJST]

Assessment reference:

[DMIN-DJST]

Assessment objective:

The assessment covers:

- a conceptual assessment of Minimise processed data.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

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

Assessment activities:

- The SHPSF'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 SHPSF'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 reference:

[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 SHPSF'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 SHPSF shall be complete:

- a list of all SHPSF's hardware architectural components:
- for each SHPSF's hardware architectural component:
  - a list of all power supplies; and
  - for each power supply:
    - a description whether the power supply can power the hardware architectural component alone; and
  - a list of all functionalities of the SHPSF that need communication involving the hardware architectural component:
  - for each of these functionalities:
    - a list of interfaces of the SHPSF, where the operational status of the hardware architectural components can be read including a description on how the operational status can be implied from the interface readings; and

- a list of interfaces of the SHPSF, 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.

The following test setups shall be prepared:

- the SHPSF is set up in default configuration; and
- a test setup to:
  - safely disconnect or disable and reconnect or enable the power supplies of the SHPSF's hardware architectural components; and
  - enable access to at least one interfaces of the SHPSF, where the operational status of the SHPSF can be read; and
  - enable access to at least one interfaces of the SHPSF, where the connection status the necessary communication channels status of the hardware architectural components can be read; and
  - (if the connection status for all necessary communication channels of the hardware architectural components cannot be read from the SHPSF) 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; and
  - wait at least 30 s; and
  - reconnect or enable the power supplies; and
  - monitor the operational status of the SHPSF; and
  - monitor the connection status for all necessary communication channels of the hardware architectural component; and
  - record the order in which the power supplies are disconnect or disable and reconnect or enable; and
    - record the time relative to the reconnection or enabling of the last power supply, after which the SHPSF 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 SHPSF has not resumed operation.

Assessment verdict:

The verdict PASS shall be assigned if:

- the SHPSF 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 SHPSF 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 reference:

[AVAI-TIME-NETW]

Assessment objective:

The assessment covers:

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

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

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

The following test setups shall be prepared:

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

Assessment activities:

The following activities shall be performed:

- verify the correctness and completeness of the documentation; and
- 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 SHPSFs architectural component; and

- wait at least 30 s; and
- 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 and record the status of the function and the disconnected or disabled communication type; and
- 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; and
- 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 reference:

[AVAI-TIME-RECO-NETW]

Assessment objective:

The assessment covers:

- a conceptual assessment of [AVAI-TIME-RECO-NETW]; and
- a functional completeness assessment on the SHPSF capabilities that are addressed by [AVAI-TIME-RECO-NETW]; and
- a functional sufficiency assessment of the SHPSFs 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 SHPSF shall be complete:

- a list of all functions of the SHPSF that need communication involving the architectural component; and
  - 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;

and

- a list of interfaces of the SHPSF, 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 SHPSF is set up in default configuration; and
- a test setup to:
  - disconnect or disable the public communication of the SHPSFs architectural component
  - disconnect or disable the adjacent communication of the SHPSFs architectural component
  - enable access to at least one interfaces of the SHPSF, 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 SHPSF:
    - 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; and
- 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 SHPSFs architectural component; and
  - wait at least 60 s; and
  - reconnect or enable the corresponding communication type and record the corresponding communication type; and
  - for each documented function:
    - monitor the operational status of the function; and
    - for each interface necessary for the operation of this function:
      - monitor the connection status; and
        - record the time relative to the reconnection or enabling of the corresponding communication type, after which the SHPSF 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 SHPSF 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 SHPSF 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 SHPSF 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 reference:

[AVAI-TIME-OUTA-NOT]

Assessment objective:

The assessment covers:

- a conceptual assessment of [AVAI-TIME-OUTA-NOT]; and
- a functional sufficiency assessment of the SHPSFs notification in case of non-availability induced by network resource restrictions, to fulfil [AVAI-TIME-OUTA-NOT]; and
- a functional sufficiency assessment of the SHPSFs 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 SHPSF shall be complete:

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

The following test setups shall be prepared:

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

Assessment activities:

The following activities shall be performed:

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

Assessment verdict:

The verdict PASS shall be assigned if:

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

and

- the SHPSF 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 SHPSF 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 reference:

[AVAI-TIME-PREV-NOT]

Assessment objective:

The assessment covers:

- a conceptual assessment of [AVAI-TIME-PREV-NOT]; and
- a functional sufficiency assessment of the SHPSFs notification in case of network resource restrictions, to fulfil [AVAI-TIME-PREV-NOT]; and
- a functional sufficiency assessment of the SHPSFs 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 SHPSF shall be complete:

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

The following test setups shall be prepared:

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

Assessment activities:

The following activities shall be performed:

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

Assessment verdict:

The verdict PASS shall be assigned if:

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

and

- the SHPSF sends notifications according to its configuration in case of network bandwidth limitation; or

- no time sensitive function with IMP.AVAI.TIME.High of the SHPSF of the SHPSF 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-NET-PRIO]

Assessment reference:

[AVAI-TIME-NET-PRIO]

Assessment objective:

The assessment covers:

- a conceptual assessment of [AVAI-TIME-NET-PRIO]; and
- a functional sufficiency assessment of the SHPSFs resource prioritization in case of non-availability induced by network resource restrictions, to fulfil [AVAI-TIME-NET-PRIO],

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- description how the status of the SHPSFs time sensitive functions can be read or deduced; and
- a list of all time sensitive functions of the SHPSF:
- for each of these functions:
  - the time sensitive availability impact class; and
  - whether the function needs network connectivity; and
- a prioritization policy for the time sensitive functions of the SHPSF in case of network resource conflict.

The following test setups shall be prepared:

- the SHPSF is set up in default configuration; and
- a test setup to:
  - read or deduced the status of the time sensitive functions from the SHPSF; and
  - limit the network bandwidth between the SHPSF's architectural component and the SHPSFs RDPS to the internet.

Assessment activities:

The following activities shall be performed:

- verify the correctness and completeness of the documentation; and
- conceptually verify the prioritization policy; and
- progressively lower the network bandwidth available to the SHPSFs architectural component and 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
- the prioritization policy is represented by the status of every time sensitive function during network bandwidth limitation.

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 reference:

[AVAI-TIME-RES-PRIO]

Assessment objective:

The assessment covers:

- a conceptual assessment of [AVAI-TIME-RES-PRIO]; and
- a functional sufficiency assessment of the SHPSFs 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 SHPSF shall be complete:

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

The following test setups shall be prepared:

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

Assessment activities:

The following activities shall be performed:

- verify the correctness and completeness of the documentation; and

- conceptually verify the prioritization policy; and
- progressively higher the intensity of requests to induce a DoS status on the SHPSF and 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
- for 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-TIME-DOS-RATE]

Assessment reference:

[AVAI-TIME-DOS-RATE]

Assessment objective:

The assessment covers:

- a conceptual assessment of [AVAI-TIME-DOS-RATE]; and
- a functional sufficiency assessment of the SHPSFs network rate limiting, to fulfil [AVAI-TIME-DOS-RATE],

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a list of all time sensitive function of the SHPSF:
- for each of these functions:
  - the time sensitive availability impact class; and
  - a list of all used interfaces; and
- a list of all machine interface provided by the SHPSF; and
- rate limiting policy for the SHPSF.

The following test setups shall be prepared:

- the SHPSF is set up in default configuration; and
- a test setup to:
  - induce a DoS status on the SHPSF causing increasing demand on processing resources; and
  - check the status of all time sensitive function with IMP.AVAI.TIME.High.

Assessment activities:

The following activities shall be performed:

- verify the correctness and completeness of the documentation; and
- progressively increase the intensity of requests to induce a DoS status on the SHPSF;
- record the status of every time sensitive function with IMP.AVAI.TIME.High

Assessment verdict:

The verdict PASS shall be assigned if:

- no indication, that the documentation is incorrect or incomplete, are found; and
- the rate limiting policy is conceptually valid; and
- for every time sensitive function with IMP.AVAI.TIME.High or higher:
  - the status of the function is in accordance with the rate limiting policy during DoS.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- descriptions of the performed tests and records of performed tests

6.10.9 Assessment criteria for [AVAI-SUM-SCHEDULE]

Assessment reference:

[AVAI-SUM-SCHEDULE]

Assessment objective:

The assessment covers:

- a conceptual assessment of [AVAI-SUM-SCHEDULE]; and
- a functional sufficiency assessment of the SHPSFs 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 SHPSF shall be complete:

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

The following test setups shall be prepared:

- the SHPSF is set up in default configuration.

Assessment activities:

The following activities shall be performed:

- verify the correctness and completeness of the documentation; and
- 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; and
  - 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

6.11.1 Assessment criteria for [NOINF-AMP]

Assessment reference:

[AVAI-TIME-NET-PRIO]

Assessment objective:

The assessment covers:

- a conceptual assessment of [AVAI-TIME-NET-PRIO]; and
- a functional sufficiency assessment of the SHPSFs network amplification, to fulfil [AVAI-TIME-NET-PRIO],

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a list of all function whose use can impact the availability of other devices, services or networks of the SHPSF; and
- for each of these functions:
  - the function whose use can impact the availability of other devices, services or networks impact class; and
  - a list of all used interfaces.

The following test setups shall be prepared:

- the SHPSF is set up in default configuration; and

- a test setup to:
  - execute amplification attacks against the SHPSF; and
  - measure the affective amplification of network traffic caused by the SHPSF.

Assessment activities:

The following activities shall be performed:

- verify the correctness and completeness of the documentation; and
- for every function whose use can impact the availability of other devices, services or networks with IMP.FH.DSN.Medium or higher:
  - progressively increase the intensity of an amplification attack against this function; and
  - measure the affective amplification of network traffic.

Assessment verdict:

The verdict PASS shall be assigned if:

- no indication, that the documentation is incorrect or incomplete, are found; and
- for every function whose use can impact the availability of other devices, services or networks with IMP.FH.DSN.Medium or higher:
  - the affective amplification of network traffic is not higher than 10.

The verdict FAIL shall be assigned otherwise.

Assessment evidence:

- descriptions of the performed tests and records of performed tests

6.12 Attack surface minimisation

6.12.1 Assessment criteria for [LAS-INVAL]

Assessment reference:

[LAS-INVAL]

Assessment objective:

The assessment covers:

- a conceptual assessment of [LAS-INVAL]; and
- a functional sufficiency assessment of the input validation mechanisms used by the SHPSF to fulfil [LAS-INVAL],

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for each SHPSF'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; and
  - a description of the SHPSF's input validation mechanisms.

The following test setups shall be prepared:

- For each SHPSF'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 SHPSF in default configuration.

Assessment activities:

- For each SHPSF's function that uses external data input, the SHPSF'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; and
    - 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 SHPSF's behaviour.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the SHPSF'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 reference:

[LAS-INSAN]

Assessment objective:

The assessment covers:

- a conceptual assessment of [LAS-INSAN]; and
- a functional sufficiency assessment of the input sanitisation mechanisms used by the SHPSF to fulfil [LAS-INSAN],

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for each SHPSF's function that uses external data input:
  - a description of the SHPSF'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 SHPSF'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 SHPSF in default configuration.

Assessment activities:

- For each SHPSF's function that uses external data input, the SHPSF'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 SHPSF's behaviour.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the SHPSF'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 reference:

[LAS-PHY-INF]

Assessment objective:

The assessment covers:

- a conceptual assessment of [LAS-PHY-INF]; and
- a functional completeness assessment on the SHPSF's capabilities that are addressed by [LAS-PHY-INF].

Assessment preparation:

The following documentation for the SHPSF 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 SHPSF'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 SHPSF'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 SHPSF'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 reference:

[LAS-LOGIC-INF]

Assessment objective:

The assessment covers:

- a conceptual assessment of [LAS-LOGIC-INF]; and
- a functional completeness assessment on the SHPSF'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 SHPSF 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 SHPSF's intended purpose.

The following test setup shall be prepared:

- a test setup for identifying logical interfaces based on a sample SHPSF 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 SHPSF'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 SHPSF.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the SHPSF'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-APP]

Assessment reference:

[LAS-APP]

Assessment objective:

The assessment covers:

- a conceptual assessment of [LAS-APP]; and
- a functional completeness assessment on the SHPSF's capabilities that are addressed by [LAS-APP],

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a list of all application software that are installed by default; and

NOTE 1: This information might be extractable from a SHPSF's SBOM.

- for each application software installed by default:
  - a justification for its necessity for the SHPSF intended purpose.

The following test setup shall be prepared:

- a test setup for identifying application software installed at the SHPSF based on a sample SHPSF in default configuration.

NOTE 2: Such a test setup can amongst others include means to identify installed application software based on inspecting the SHPSF's interfaces and application software discovery tool results such as software binary analysis tools or source code analysis tools.

Assessment activities:

- The SHPSF's conformity to [LAS-APP] shall be validated based on the documentation.
- The correctness and completeness of the documentation shall be verified by inspecting the SHPSF.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the SHPSF's conformity to [LAS-APP]; 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 application software discovery tool results
- screenshots/logs of discovery attempts for installed application software via the SHPSF's interfaces

6.12.6 Assessment criteria for [LAS-SBOOT]

Assessment reference:

[LAS-SBOOT]

Assessment objective:

The assessment covers:

- a conceptual assessment of [LAS-SBOOT]; and
- a functional sufficiency assessment of the bootloader function used by the SHPSF to fulfil [LAS-SBOOT],

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- SBOM of the SHPSF's hardware architectural component including information on which software's integrity and authenticity is protected by the bootloader function; and
- 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 SHPSF'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 SHPSF'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 SHPSF's conformity to [LAS-SBOOT]; and
- the SHPSF'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 reference:

[PRIV-DATA-HIGH]

Assessment objective:

The assessment covers:

- a conceptual assessment of [PRIV-DATA-HIGH]; and
- a functional sufficiency assessment of the SHPSF's mechanisms that ensure conformity with [PRIV-DATA-HIGH].

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a list of the SHPSF's architectural components; and
- for each SHPSF'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 SHPSF's intended purpose; and
  - 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 unauthorised processes running on the same hardware.

Assessment activities:

- The SHPSF'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 unauthorised processes.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the SHPSF'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 reference:

[PRIV-FUNC-HIGH]

Assessment objective:

The assessment covers:

- a conceptual assessment of [PRIV-FUNC-HIGH]; and
- a functional sufficiency assessment of the SHPSF's mechanisms that ensure conformity with [PRIV-FUNC-HIGH].

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a list of the SHPSF's architectural components; and
- for each SHPSF's architectural component:
  - a list of provided function assets that are:
    - time sensitive function of [IMP.AVAI.TIME.High], or
    - integrity relevant function of [IMP.INT.High], or
    - function whose use can cause harm of [IMP.FH.High]; and

- 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 SHPSF's intended purpose; and
- 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 unauthorised processes running on the same hardware.

Assessment activities:

- The SHPSF'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 unauthorised processes.

Assessment verdict:

The verdict PASS shall be assigned if:

- the documentation indicates the SHPSF'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 reference:

[MON-LOW]

Assessment objective:

The assessment covers:

- a conceptual assessment of [MON-LOW]; and
- a functional sufficiency assessment of monitoring mechanisms used by the SHPSF to fulfil [MON-LOW],

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- list of all monitoring mechanisms; and
- documentation on how the monitoring mechanisms creates audit event data; and

- 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]; and
- monitoring mechanism are enabled on the SHPSF such that at least all the events in [MON-LOW] are covered; and
- 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; and
- trigger the events listed in *Assessment preparation*; and
- 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 reference:

[MON-MEDIUM]

Assessment objective:

The assessment covers:

- a conceptual assessment of [MON-MEDIUM]; and
- a functional sufficiency assessment of monitoring mechanisms used by the SHPSF to fulfil [MON-MEDIUM],

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- list of all monitoring mechanisms; and
- documentation on how the monitoring mechanisms creates audit event data; and
- 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]; and
- 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; and
- trigger the events listed in *Assessment preparation*; and
- 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 reference:

[MON-HIGH]

Assessment objective:

The assessment covers:

- a conceptual assessment of [MON-HIGH]; and
- a functional sufficiency assessment of monitoring mechanisms used by the SHPSF to fulfil [MON-HIGH],

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- list of all monitoring mechanisms; and
- documentation on how the monitoring mechanisms creates audit event data; and
- 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]; and
- 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; and
- trigger the events listed in *Assessment preparation*; and
- 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 reference:

[MON-HANDLE]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of each audit event data generated by a monitoring mechanism of the SHPSF to fulfil [MON-HANDLE],

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for each architectural component:
  - documentation on support of public communication; and
  - 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; and
  - access the storage location where logging data is stored; and
- for each data transfer mechanism in *assessment preparation*, a test setup that allows to:
  - generate audit event data; and
  - 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; and
  - generate audit event data; and
  - check that the logging data produced by the logging mechanism from the audit event data is generated and stored; and

- 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; and
  - verify that the assigned data transfer mechanism is enabled; and
  - 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 SHPSF's conformity with [MON-HANDLE]; and
- 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; and:
  - 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 reference:

[LOG-TIME]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of logging mechanisms used by the SHPSF to fulfil [LOG-TIME],

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- documentation on how the logging mechanisms creates logging data; and
- documentation for which events logging data are created by which logging mechanism; and
- documentation on where logging data are stored; and
- 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; and
- logging mechanism are enabled on the SHPSF such that at least all the events in the following point are covered; and
- 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; and
  - for each event triggered: verify that the logging data contains a timestamp; and
- 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 reference:

[LOG-TIME-HIGH]

Assessment objective:

The assessment covers:

- a conceptual assessment of [LOG-TIME-HIGH]; and
- a functional sufficiency assessment of logging mechanisms used by the SHPSF to fulfil [LOG-TIME-HIGH],

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- documentation on how the logging mechanisms creates logging data; and
- documentation for which events logging data are created by which logging mechanism; and
- documentation on where logging data are stored; and
- 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; and
- logging mechanism are enabled on the SHPSF such that at least all the events in the following point are covered; and
- 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; and
- trigger the events listed in *Assessment preparation* and note the time; and
  - 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 reference:

[LOG-STORE-MEDIUM]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of logging mechanisms used by the SHPSF to fulfil [LOG-STORE-MEDIUM],

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF 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; and
  - documentation on how the corresponding logging mechanism generates logging data; and
  - documentation on where logging data are stored; and
  - 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; and
- logging mechanisms are enabled on the SHPSF such that at least all the events listed in [LOG-STORE-MEDIUM] (clause 5.14.2) are covered; and
- 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; and
  - trigger the generation of the audit event data; and
  - 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 reference:

[LOG-STORE-HIGH]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of logging mechanisms used by the SHPSF to fulfil [LOG-STORE-HIGH],

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF 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; and
  - documentation on how the corresponding logging mechanism generates logging data; and
  - documentation on where logging data are stored; and
  - 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; and

- logging mechanisms are enabled on the SHPSF such that at least all the events listed in [LOG-STORE-HIGH] (clause 5.14.3) are covered; and
- 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; and
  - trigger the generation of the audit event data; and
  - 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 reference:

[LOG-CONFIG]

Assessment objective:

The assessment covers:

- a conceptual assessment of [LOG-CONFIG],
- a functional sufficiency assessment of each logging mechanism used by the SHPSF to fulfil [LOG-CONFIG]

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a description of each logging mechanism, including:
  - which audit event data can be processed; and
  - which logging data are generated; and
  - where the generated logging data is stored; and

- where and how to disable the {SupportingFunctionality:LoggingMechanism}.

The following test setups shall be prepared:

- a test setup that allows to identify logging mechanisms on a sample SHPSF in default configuration; and
- for each logging mechanism, a test setup that allows to:
  - generate audit event data; and
  - access the storage location where logging data is stored; and
  - see the user interaction steps (e.g. menu, dialog, confirmation after deletion).

Assessment activities:

The following activities shall be performed:

- The SHPSF'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; and
  - check that corresponding logging data is generated (and stored) by the logging mechanism; and
  - 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 SHPSF's conformity with [LOG-CONFIG]; and
- the verification of the correctness of the documentation was successful; and
- all logging mechanisms 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 reference:

[DLM-PERM]

Assessment objective:

The assessment covers:

- a conceptual assessment of [DLM-PERM]; and
- a functional completeness assessment on the SHPSF's capabilities that are addressed by [DLM-PERM]; and
- a functional sufficiency assessment of each deletion mechanism used by the SHPSF to fulfil [DLM-PERM],

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- a description of each deletion mechanism, including:
  - deletion scope (i.e. describing what can be deleted by this mechanism); and
  - method of deletion (e.g. overwriting, access control, changing pointer address, …); and
  - method of user interaction and initiation steps; and
  - whether confirmation is provided after deletion is performed; and
  - 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 SHPSF in default configuration; and
- for each deletion mechanism, a test setup that allows to:
  - create representative user-related data and install applications; and
  - 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 SHPSF'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; and
  - 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; and
    - deletion mechanism is easy to use with limited technical knowledge; and
    - 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 SHPSF'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 SHPSF to delete all generated user-related data and applications

Annex A (informative): Relationship between the present document and the essential cybersecurity 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] final to provide one voluntary means of conforming to the requirements of Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) [i.1].

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

Table A.1: Relationship between the present document and the requirements of Regulation (EU) 2024/2847 [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 [AUM-FH] 5.6.2, 6.6.2 [AUTHZ-LP] 5.6.3, 6.6.3 [AUTHZ-R] 5.6.4, 6.6.4 [AVAI-TIME-RECO-POW] 5.10.1, 6.10.1 [AVAI-TIME-NETW] 5.10.2, 6.10.2 [AVAI-TIME-RECO-NETW] 5.10.3, 6.10.3 [AVAI-TIME-OUTA-NOT] 5.10.4, 6.10.4 [AVAI-TIME-PREV-NOT] 5.10.5, 6.10.5 [AVAI-TIME-NET-PRIO] 5.10.6, 6.10.6 [AVAI-TIME-RES-PRIO] 5.10.7, 6.10.7 [AVAI-TIME-DOS-RATE] 5.10.8, 6.10.8 [AVAI-SUM-SCHEDULE] 5.10.9, 6.10.9 [BACKUP-TRANS] 5.2.4, 6.2.4 [BACKUP-AUTOTRANS] 5.2.5, 6.2.5 [BACKUP-EXPORT] 5.2.6, 6.2.6 [CONF-SSM] 5.7.1, 6.7.1 [CONF-COM] 5.7.2, 6.7.2 [CRY-GENERAL] 5.4.6, 6.4.6 [CRY-CCK-PRE-LEN] 5.4.7, 6.4.7 [CRY-CCK-GEN] 5.4.8, 6.4.8 [CRY-PW-PRE-COM] 5.4.9, 6.4.9 [CRY-PW-GEN-COM] 5.4.0, 6.4.10 [CRY-PW-USR-COM] 5.4.1, 6.4.11 [DLM-PERM] 5.15.1, 6.15.1 [DMIN-DJST] 5.9.1, 6.9.1 [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 [PRIV-FUNC-HIGH] 5.13.2, 6.13.2 [GUI-SECCONF] 5.2.3, 6.2.3 [INT-SSM] 5.8.1, 6.8.1 [INT-COM] 5.8.2, 6.8.2 [INT-SWPCK] 5.8.3, 6.8.3 [LAS-INVAL] 5.12.1, 6.12.1 [LAS-INSAN] 5.12.2, 6.12.2 [LAS-PHY-INF] 5.12.3, 6.12.3 [LAS-LOGIC-INF] 5.12.4, 6.12.4 [LAS-APP] 5.12.5, 6.12.5 [LAS-SBOOT] 5.12.6, 6.12.6 [MON-LOW] 5.14.1, 6.14.1 [MON-MEDIUM] 5.14.2, 6.14.2 [MON-HIGH] 5.14.3, 6.14.3 [MON-HANDLE] 5.14.4, 6.14.4 [LOG-TIME] 5.14.5, 6.14.5 [LOG-TIME-HIGH] 5.14.6, 6.14.6 [LOG-STORE-MEDIUM] 5.14.7, 6.14.7 [LOG-STORE-HIGH] 5.14.8, 6.14.8 [LOG-CONFIG] 5.14.9, 6.14.9 [NKEV-MKAV] 5.3.1, 6.3.1 [NKEV-INIT-UDP] 5.3.2, 6.3.2 [NOINF-AMP] 5.11.1, 6.11.1 [SDC-AUM-FH] 5.4.1, 6.4.1 [SDC-SUM-AUTO] 5.4.2, 6.4.2 [SDC-SUM-NOTIF] 5.4.3, 6.4.3 [SDC-FRM] 5.4.4, 6.4.4 [SDC-MON-HANDLE] 5.4.5, 6.4.5 [SU-SUPPORT] 5.5.1, 6.5.1 [SU-PROVIDE] 5.5.2, 6.5.2 [SU-AUTO] 5.5.3, 6.5.3 [SU-DISABLE-AUTO] 5.5.4, 6.5.4 [SU-POSTPONE-AUTO] 5.5.5, 6.5.5 [SU-NOTIF] 5.5.6, 6.5.6 [USERNOT-NOSECFUC] 5.2.1, 6.2.1 [USERNOT-SECREL] 5.2.2, 6.2.2	
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 [NKEV-INIT-UDP] 5.3.2, 6.3.2	

Description	Essential Requirements of Regulation (EU) 2024/2847	Clause(s) of the present document	Remarks / Notes
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-GENERAL] 5.4.6, 6.4.6 [CRY-CCK-PRE-LEN] 5.4.7, 6.4.7 [CRY-CCK-GEN] 5.4.8, 6.4.8 [CRY-PW-PRE-COM] 5.4.9, 6.4.9 [CRY-PW-GEN-COM] 5.4.0, 6.4.10 [CRY-PW-USR-COM] 5.4.1, 6.4.11 [LAS-LOGIC-INF] 5.12.4, 6.12.4 [LAS-APP] 5.12.5, 6.12.5 [SDC-AUM-FH] 5.4.1, 6.4.1 [SDC-SUM-AUTO] 5.4.2, 6.4.2 [SDC-SUM-NOTIF] 5.4.3, 6.4.3 [SDC-FRM] 5.4.4, 6.4.4 [SDC-MON-HANDLE] 5.4.5, 6.4.5	
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 [SDC-SUM-NOTIF] 5.4.3, 6.4.3 [SU-SUPPORT] 5.5.1, 6.5.1 [SU-PROVIDE] 5.5.2, 6.5.2 [SU-AUTO] 5.5.3, 6.5.3 [SU-DISABLE-AUTO] 5.5.4, 6.5.4 [SU-POSTPONE-AUTO] 5.5.5, 6.5.5 [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 [AUM-FH] 5.6.2, 6.6.2 [AUTHZ-LP] 5.6.3, 6.6.3 [AUTHZ-R] 5.6.4, 6.6.4 [MON-MEDIUM] 5.14.2, 6.14.2 [MON-HIGH] 5.14.3, 6.14.3 [LOG-TIME] 5.14.5, 6.14.5 [LOG-TIME-HIGH] 5.14.6, 6.14.6 [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 [AUM-FH] 5.6.2, 6.6.2 [AUTHZ-LP] 5.6.3, 6.6.3 [AUTHZ-R] 5.6.4, 6.6.4 [CONF-SSM] 5.7.1, 6.7.1 [CONF-COM] 5.7.2, 6.7.2	
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 [AUM-FH] 5.6.2, 6.6.2 [AUTHZ-LP] 5.6.3, 6.6.3 [AUTHZ-R] 5.6.4, 6.6.4 [INT-SSM] 5.8.1, 6.8.1 [INT-COM] 5.8.2, 6.8.2 [INT-SWPCK] 5.8.3, 6.8.3 [MON-LOW] 5.14.1, 6.14.1 [MON-MEDIUM] 5.14.2, 6.14.2 [MON-HIGH] 5.14.3, 6.14.3	
Annex I, Part I, (2)(g)	"Products with digital elements process only data, personal or	[DMIN-DJST] 5.9.1, 6.9.1	

Description	Essential Requirements of Regulation (EU) 2024/2847	Clause(s) of the present document	Remarks / Notes
	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)."		
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 [AVAI-TIME-NETW] 5.10.2, 6.10.2 [AVAI-TIME-RECO-NETW] 5.10.3, 6.10.3 [AVAI-TIME-OUTA-NOT] 5.10.4, 6.10.4 [AVAI-TIME-PREV-NOT] 5.10.5, 6.10.5 [AVAI-TIME-NET-PRIO] 5.10.6, 6.10.6 [AVAI-TIME-RES-PRIO] 5.10.7, 6.10.7 [AVAI-TIME-DOS-RATE] 5.10.8, 6.10.8 [AVAI-SUM-SCHEDULE] 5.10.9, 6.10.9	
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."	[NOINF-AMP] 5.11.1, 6.11.1	
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 [LAS-INSAN] 5.12.2, 6.12.2 [LAS-PHY-INF] 5.12.3, 6.12.3 [LAS-LOGIC-INF] 5.12.4, 6.12.4 [LAS-APP] 5.12.5, 6.12.5 [LAS-SBOOT] 5.12.6, 6.12.6	
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 [AVAI-TIME-NET-PRIO] 5.10.6, 6.10.6 [AVAI-TIME-RES-PRIO] 5.10.7, 6.10.7 [PRIV-DATA-HIGH] 5.13.1, 6.13.1 [PRIV-FUNC-HIGH] 5.13.2, 6.13.2	
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 [MON-MEDIUM] 5.14.2, 6.14.2 [MON-HIGH] 5.14.3, 6.14.3 [MON-HANDLE] 5.14.4, 6.14.4 [LOG-TIME] 5.14.5, 6.14.5 [LOG-TIME-HIGH] 5.14.6, 6.14.6 [LOG-STORE-MEDIUM] 5.14.7, 6.14.7 [LOG-STORE-HIGH] 5.14.8, 6.14.8 [LOG-CONFIG] 5.14.9, 6.14.9 [SDC-MON-HANDLE] 5.4.5, 6.4.5 [SU-DISABLE-AUTO] 5.5.4, 6.5.4 [SU-POSTPONE-AUTO] 5.5.5, 6.5.5	

Description	Essential Requirements of Regulation (EU) 2024/2847	Clause(s) of the present document	Remarks / Notes
		[SU-NOTIF] 5.5.6, 6.5.6 [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 [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 is based on.

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 4.1.1.

The data assets addressed by the present document are listed in clause 4.1.2.

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 clause 4.1. The impact class assignment is provided in clause 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 SHPSFs 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 SHPSF		**Prevention**: [ACM-FH] 5.6.1 [AUM-FH] 5.6.2 [AUTHZ-LP] 5.6.3 [AUTHZ-R] 5.6.4 [PRIV-FUNC-HIGH] 5.13.2 [LAS-PHY-INF] 5.12.3 [LAS-LOGIC-INF] 5.12.4 [LAS-APP] 5.12.5 [NOINF-AMP] 5.11.1 [SDC-AUM-FH] 5.4.1 **Information**: [MON-LOW] 5.14.1 [MON-MEDIUM] 5.14.2 [MON-HIGH] 5.14.3 [MON-HANDLE] 5.14.4 [LOG-TIME] 5.14.5 [LOG-TIME-HIGH] 5.14.6 [LOG-STORE-MEDIUM] 5.14.7 [LOG-STORE-HIGH] 5.14.8 [LOG-CONFIG] 5.14.9 [SDC-MON-HANDLE] 5.4.5 [USERNOT-NOSECFUC] 5.2.1 **Restoration**: [SDC-FRM] 5.4.4	COM, IF and POE	C
[2]	A threat actor	tampers	integrity relevant data	permanently stored on the SHPSF		**Prevention**: [PRIV-DATA-HIGH] 5.13.1 [INT-SSM] 5.8.1		C
[3]	A threat actor	tampers	integrity relevant data	volatile stored on the SHPSF		**Prevention**: [PRIV-DATA-HIGH] 5.13.1		C
[4]	A threat actor	tampers	integrity relevant data	communicated from or to the architectural component		**Prevention**: [INT-COM] 5.8.2	COM, IF and POE	C

No.	Threat Actor	Threat action	Asset (relevant impact parameter)	Threat details		Requirement(s) for mitigation	Relevant attack surface parameter	Risk coverage
[5]	A threat actor	discloses	confidential data	on the SHPSF	unnecessarily processed	**Prevention**: [DMIN-DJST] 5.9.1		C
[6]	A threat actor	discloses	confidential data	permanently stored on the SHPSF	during storage	**Prevention**: [CONF-SSM] 5.7.1 [PRIV-DATA-HIGH] 5.13.1	POE	C
[7]	A threat actor	discloses	confidential data	permanently stored on the SHPSF	after deletion	**Prevention**: [DLM-PERM] 5.15.1		C
[8]	A threat actor	discloses	confidential data	volatile stored on the SHPSF	during usage	**Prevention**: [PRIV-DATA-HIGH] 5.13.1		C
[9]	A threat actor	discloses	confidential data	volatile stored on the SHPSF	after usage	**Prevention**: [PRIV-DATA-HIGH] 5.13.1		C
[10]	A threat actor	discloses	confidential data	communicated from or to the architectural component		**Prevention**: [CONF-COM] 5.7.2	COM, IF and POE	C
[12]	A threat actor	tampers	integrity relevant function	on the SHPSF		**Prevention**: [PRIV-DATA-HIGH] 5.13.1 [PRIV-FUNC-HIGH] 5.13.2 [INT-SWPCK] 5.8.3 [LAS-SBOOT] 5.12.6		C
[13]	A threat actor	impacts the availability of	time sensitive function	on the SHPSF	by interruption caused by a software update installation	**Prevention**: [AVAI-SUM-SCHEDULE] 5.10.9		C
[14]	A threat actor	impacts the availability of	time sensitive function	on the SHPSF	by interruption of power supply	**Information**: [AVAI-TIME-OUTA-NOT] 5.10.4 [AVAI-TIME-PREV-NOT] 5.10.5 **Restoration**: [AVAI-TIME-RECO-POW] 5.10.1		C

No.	Threat Actor	Threat action	Asset (relevant impact parameter)	Threat details		Requirement(s) for mitigation	Relevant attack surface parameter	Risk coverage
[15]	A threat actor	impacts the availability of	time sensitive function	on the SHPSF	by interruption of network connection	**Prevention**: [AVAI-TIME-NETW] 5.10.2 **Information**: [AVAI-TIME-OUTA-NOT] 5.10.4 [AVAI-TIME-PREV-NOT] 5.10.5 **Restoration**: [AVAI-TIME-RECO-NETW] 5.10.3		C
[16]	A threat actor	impacts the availability of	time sensitive function	on the SHPSF	due to overloading of a resource or connection	**Prevention**: [AVAI-TIME-NET-PRIO] 5.10.6 [AVAI-TIME-RES-PRIO] 5.10.7 [AVAI-TIME-DOS-RATE] 5.10.8 **Information**: [AVAI-TIME-OUTA-NOT] 5.10.4	IF	C
[17]	A threat actor	exploits an implementation vulnerability to compromise	a product cybersecurity asset			**Prevention**: [PRIV-DATA-HIGH] 5.13.1 [PRIV-FUNC-HIGH] 5.13.2 [LAS-INVAL] 5.12.1 [LAS-INSAN] 5.12.2 [NKEV-MKAV] 5.3.1 **Information**: [NKEV-INIT-UDP] 5.3.2 [SDC-SUM-NOTIF] 5.4.3 [SU-DISABLE-AUTO] 5.5.4 [SU-POSTPONE-AUTO] 5.5.5 [SU-NOTIF] 5.5.6 **Restoration**: [NKEV-INIT-UDP] 5.3.2 [SDC-SUM-AUTO] 5.4.2 [SU-SUPPORT] 5.5.1 [SU-PROVIDE] 5.5.2 [SU-AUTO] 5.5.3		C

No.	Threat Actor	Threat action	Asset (relevant impact parameter)	Threat details		Requirement(s) for mitigation	Relevant attack surface parameter	Risk coverage
[18]	A user	unconsciously performs an incorrect actions		on the SHPSF		**Prevention**: [GUI-SECCONF] 5.2.3 **Information**: [GUI-SECCONF] 5.2.3	IF.Human	C
[19]	A user	performs insecure actions		on the SHPSF	because the user is not aware of security relevant information	**Prevention**: [USERNOT-SECREL] 5.2.2 **Information**: [USERNOT-SECREL] 5.2.2	IF.Human	C
[20]	An incident	results in a permanent loss of	loss sensitive data	permanently stored on the SHPSF		**Prevention**: [BACKUP-TRANS] 5.2.4 [BACKUP-AUTOTRANS] 5.2.5 [BACKUP-EXPORT] 5.2.6		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 SHPSF assets provided in clause D.

B.7.2 Confidential data

confidentiality impact class low (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 SHPSF.

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 SHPSF or a limited number of other products; or
- additional or increased attack opportunities over a prolonged time limited to non-key-functionalities on the SHPSF.

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 SHPSF or a limited number of other products; or
- additional or increased attack opportunities over a short time on a significant number of other products.

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-key-functionalities on the SHPSF 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 key-functionalities of the SHPSF over a short time; or
- non-availability of non-key-functionalities on the SHPSF 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 key-functionalities of the SHPSF for a prolonged time; or
- permanent non-availability of non-key-functionalities of the SHPSF.

B.7.4 Time sensitive function

time sensitive availability impact class low (IMP.AVAI.TIME.Low):

The delay of availability may lead to:

- non-availability of non-key-functionalities on the SHPSF for a short time.

time sensitive availability impact class medium (IMP.AVAI.TIME.Medium):

The delay of availability may lead to:

- non-availability of key-functionalities on the SHPSF for a short time; or
- non-availability of non-key-functionalities on the SHPSF for a prolonged time.

time sensitive availability impact class high (IMP.AVAI.TIME.High):

The delay of availability may lead to:

- non-availability of key-functionalities of the SHPSF for a prolonged time; or
- permanent non-availability of non-key-functionalities of the SHPSF.

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 SHPSF; or
- non-availability of non-key-functionalities on the SHPSF 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 SHPSF or a limited number of other products;
- additional or increased attack opportunities over a prolonged time limited to non-key-functionalities on the SHPSF; or
- non-availability of key-functionalities on the SHPSF for a short time; or
- non-availability of non-key-functionalities on the SHPSF 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 SHPSF or a limited number of other products;
- additional or increased attack opportunities for a short time on a significant number of other products;
- non-availability of key-functionalities of the SHPSF for a prolonged time; or
- permanent non-availability of non-key-functionalities of the SHPSF.

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

Where no use case specific impact class assignment is provided by the present document, the impact classes shall be assigned to data assets in accordance with table D.1.

Table D.1: Mapping of specific data assets to impact classes for generic data asset categories

Specific data asset	Impact class for data asset categories		
	Impact class for confidential SHPSF data	**Impact class for integrity relevant SHPSF data**	**Impact class for loss critical availability relevant SHPSF data**
actuator control data	NO	IMP.INT = Maximum(IMP.FH of controlled actuator control function)	IMP.AVAI.LOSS.LOW
audit event data	IMP.CONF = Maximum(IMP.CONF of confidential data contained in the audit event data)	IMP.INT = Maximum(IMP.FH of SHPSFs functions using audit event data)	IMP.AVAI.LOSS.MEDIUM
authorisation policy data	IMP.CONF.MEDIUM	IMP.INT.HIGH	IMP.AVAI.LOSS.LOW
battery status data	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.LOW
cryptographic security parameter	IMP.CONF = Maximum(Maximum(IMP.CONF, IMP.INT of all data assets whose protection relies on the confidentiality of the cryptographic security parameter),Maximum(IMP.INT, IMP.FH of all function assets whose protection relies on the confidentiality of the cryptographic security parameter))	IMP.INT = Maximum(Maximum(IMP.CONF, IMP.INT of all data assets whose protection relies on the integrity of the cryptographic security parameter),Maximum(IMP.INT, IMP.FH of all function assets whose protection relies on the integrity of the cryptographic security parameter))	IMP.AVAI.LOSS = Maximum(IMP.AVAI.LOSS of all data assets which are lost when the cryptographic security parameter is lost)
device identifier data	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.LOW
entity's location data	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
fire detection data	IMP.CONF.LOW	IMP.INT.HIGH	IMP.AVAI.LOSS.LOW
function binary data	NO	IMP.INT = Maximum(IMP.FH, IMP.INT, IMP.AVAI.TIME of function it implements)	NO
function configuration data	NO	IMP.INT = Maximum(IMP.INT, IMP.AVAI.TIME, IMP.FH of configured function)	IMP.AVAI.LOSS = Maximum(IMP.AVAI.TIME of configured function)
function fault detection data	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.LOW
health data	IMP.CONF.HIGH	IMP.INT.HIGH	IMP.AVAI.LOSS.MEDIUM
hold-up detection data	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.LOW
human emergency detection data	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.LOW
identity data for authentication	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.LOW
inflammable/explosive gas detection data	IMP.CONF.LOW	IMP.INT.HIGH	IMP.AVAI.LOSS.LOW
intrusion detection data	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.LOW

Specific data asset	Impact class for data asset categories		
	Impact class for confidential SHPSF data	**Impact class for integrity relevant SHPSF data**	**Impact class for loss critical availability relevant SHPSF data**
locking element position data	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.LOW
logging data	IMP.CONF = Maximum(IMP.CONF of confidential data contained in the logging data)	IMP.INT = Maximum(IMP.FH of SHPSFs functions using logging data)	IMP.AVAI.LOSS.MEDIUM
network status data	IMP.CONF.LOW	IMP.INT.MEDIUM	IMP.AVAI.LOSS.LOW
object tamper detection data	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.LOW
other products' function configuration data	IMP.CONF = Maximum(IMP.FH of other products' configured functions)	IMP.INT = Maximum(IMP.FH, IMP.INT, IMP.AVAI.TIME of other products' configured functions)	IMP.AVAI.LOSS = Maximum(IMP.AVAI.TIME of other products' configured functions)
personal contact data	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
personal notes data	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
private audio data	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
private video data	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
public data asset	IMP.CONF.LOW	IMP.INT.MEDIUM	NO
real-time data	NO	IMP.INT.MEDIUM	NO
SHPSF tamper detection data	IMP.CONF.MEDIUM	IMP.INT = Maximum(IMP.INT of architectural component's functions)	IMP.AVAI.LOSS.LOW
software package	IMP.CONF = Maximum(IMP.CONF of confidential data contained in the package)	IMP.INT = Maximum(IMP.INT of SHPSF's integrity relevant function)	NO
state data	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.LOW
window/door opening status data	IMP.CONF.LOW	IMP.INT.MEDIUM	IMP.AVAI.LOSS.LOW

For the specific use cases defined in clause 4.6.2, the corresponding table (tables D.2, D.3, D.4, D.5) shall be used to assign impact classes to data asset.

Table D.2: Mapping of specific data assets to impact classes for generic data asset categories for BIS use case

Specific data asset	Impact class for data asset categories		
	Impact class for confidential SHPSF data	**Impact class for integrity relevant SHPSF data**	**Impact class for loss critical availability relevant SHPSF data**
actuator control data for BIS	IMP.CONF.LOW	IMP.INT = Maximum(IMP.FH of controlled actuator control function)	IMP.AVAI.LOSS.MEDIUM
cryptographic security parameter for BIS	IMP.CONF = Maximum(Maximum(IMP.CONF, IMP.INT of all data assets whose protection relies on the confidentiality of the cryptographic security parameter),Maximum(IMP.INT, IMP.FH of all function assets whose protection relies on the confidentiality of the cryptographic security parameter))	IMP.INT = Maximum(Maximum(IMP.CONF, IMP.INT of all data assets whose protection relies on the integrity of the cryptographic security parameter),Maximum(IMP.INT, IMP.FH of all function assets whose protection relies on the integrity of the cryptographic security parameter))	IMP.AVAI.LOSS = Maximum(IMP.AVAI.LOSS of all data assets which are lost when the cryptographic security parameter is lost)
device identifier data for BIS	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
entity's location data for BIS	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
function binary data for BIS	NO	IMP.INT = Maximum(IMP.FH, IMP.INT, IMP.AVAI.TIME of function it implements)	NO
function configuration data for BIS	IMP.CONF.MEDIUM	IMP.INT = Maximum(IMP.INT, IMP.AVAI.TIME, IMP.FH of configured function)	IMP.AVAI.LOSS = Maximum(IMP.AVAI.TIME of configured function)
function fault detection data for BIS	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.LOW
identity data for authentication for BIS	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
logging data for BIS	IMP.CONF = Maximum(IMP.CONF of confidential data contained in the logging data)	IMP.INT = Maximum(IMP.FH of SHPSFs functions using logging data)	IMP.AVAI.LOSS.MEDIUM
object tamper detection data for BIS	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
personal contact data for BIS	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
private audio data for BIS	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
private video data for BIS	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
real-time data for BIS	IMP.CONF.LOW	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
SHPSF tamper detection data for BIS	IMP.CONF.MEDIUM	IMP.INT = Maximum(IMP.INT of architectural component's functions)	IMP.AVAI.LOSS.MEDIUM
state data for BIS	IMP.CONF.LOW	IMP.INT.LOW	IMP.AVAI.LOSS.LOW
window/door opening status data for BIS	IMP.CONF.LOW	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM

Table D.3: Mapping of specific data assets to impact classes for generic data asset categories for FGS use case

Specific data asset	Impact class for data asset categories		
	Impact class for confidential SHPSF data	**Impact class for integrity relevant SHPSF data**	**Impact class for loss critical availability relevant SHPSF data**
actuator control data for FGS	IMP.CONF.LOW	IMP.INT = Maximum(IMP.FH of controlled actuator control function)	IMP.AVAI.LOSS.MEDIUM
battery status data for FGS	IMP.CONF.LOW	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
cryptographic security parameter for FGS	IMP.CONF = Maximum(Maximum(IMP.CONF, IMP.INT of all data assets whose protection relies on the confidentiality of the cryptographic security parameter),Maximum(IMP.INT, IMP.FH of all function assets whose protection relies on the confidentiality of the cryptographic security parameter))	IMP.INT = Maximum(Maximum(IMP.CONF, IMP.INT of all data assets whose protection relies on the integrity of the cryptographic security parameter),Maximum(IMP.INT, IMP.FH of all function assets whose protection relies on the integrity of the cryptographic security parameter))	IMP.AVAI.LOSS = Maximum(IMP.AVAI.LOSS of all data assets which are lost when the cryptographic security parameter is lost)
device identifier data for FGS	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.LOW
fire detection data for FGS	IMP.CONF.LOW	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
function binary data for FGS	NO	IMP.INT = Maximum(IMP.FH, IMP.INT, IMP.AVAI.TIME of function it implements)	NO
function configuration data for FGS	IMP.CONF.LOW	IMP.INT = Maximum(IMP.INT, IMP.AVAI.TIME, IMP.FH of configured function)	IMP.AVAI.LOSS = Maximum(IMP.AVAI.TIME of configured function)
function fault detection data for FGS	IMP.CONF.LOW	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
identity data for authentication for FGS	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.LOW
inflammable/explosive gas detection data for FGS	IMP.CONF.LOW	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
logging data for FGS	IMP.CONF = Maximum(IMP.CONF of confidential data contained in the logging data)	IMP.INT = Maximum(IMP.FH of SHPSFs functions using logging data)	IMP.AVAI.LOSS.MEDIUM
other products' function configuration data for FGS	IMP.CONF = Maximum(IMP.FH of other products' configured functions)	IMP.INT = Maximum(IMP.FH, IMP.INT, IMP.AVAI.TIME of other products' configured functions)	IMP.AVAI.LOSS = Maximum(IMP.AVAI.TIME of other products' configured functions)
real-time data for FGS	IMP.CONF.LOW	IMP.INT.LOW	IMP.AVAI.LOSS.LOW
state data for FGS	IMP.CONF.LOW	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM

Table D.4: Mapping of specific data assets to impact classes for generic data asset categories for I&HAS use case

Specific data asset	Impact class for data asset categories		
	Impact class for confidential SHPSF data	**Impact class for integrity relevant SHPSF data**	**Impact class for loss critical availability relevant SHPSF data**
actuator control data for I&HAS	IMP.CONF.MEDIUM	IMP.INT = Maximum(IMP.FH of controlled actuator control function)	IMP.AVAI.LOSS.MEDIUM
battery status data for I&HAS	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
cryptographic security parameter for I&HAS	IMP.CONF = Maximum(Maximum(IMP.CONF, IMP.INT of all data assets whose protection relies on the confidentiality of the cryptographic security parameter),Maximum(IMP.INT, IMP.FH of all function assets whose protection relies on the confidentiality of the cryptographic security parameter))	IMP.INT = Maximum(Maximum(IMP.CONF, IMP.INT of all data assets whose protection relies on the integrity of the cryptographic security parameter),Maximum(IMP.INT, IMP.FH of all function assets whose protection relies on the integrity of the cryptographic security parameter))	IMP.AVAI.LOSS = Maximum(IMP.AVAI.LOSS of all data assets which are lost when the cryptographic security parameter is lost)
device identifier data for I&HAS	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.LOW
function binary data for I&HAS	NO	IMP.INT = Maximum(IMP.FH, IMP.INT, IMP.AVAI.TIME of function it implements)	NO
function configuration data for I&HAS	IMP.CONF.MEDIUM	IMP.INT = Maximum(IMP.INT, IMP.AVAI.TIME, IMP.FH of configured function)	IMP.AVAI.LOSS = Maximum(IMP.AVAI.TIME of configured function)
function fault detection data for I&HAS	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
hold-up detection data for I&HAS	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
identity data for authentication for I&HAS	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.LOW
intrusion detection data for I&HAS	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
logging data for I&HAS	IMP.CONF = Maximum(IMP.CONF of confidential data contained in the logging data)	IMP.INT = Maximum(IMP.FH of SHPSFs functions using logging data)	IMP.AVAI.LOSS.MEDIUM
object tamper detection data for I&HAS	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
other products' function configuration data for I&HAS	IMP.CONF = Maximum(IMP.FH of other products' configured functions)	IMP.INT = Maximum(IMP.FH, IMP.INT, IMP.AVAI.TIME of other products' configured functions)	IMP.AVAI.LOSS = Maximum(IMP.AVAI.TIME of other products' configured functions)
private audio data for I&HAS	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
private video data for I&HAS	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
real-time data for I&HAS	IMP.CONF.LOW	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
SHPSF tamper detection data for I&HAS	IMP.CONF.MEDIUM	IMP.INT = Maximum(IMP.INT of architectural component's functions)	IMP.AVAI.LOSS.LOW
state data for I&HAS	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
window/door opening status data for I&HAS	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM

Table D.5: Mapping of specific data assets to impact classes for generic data asset categories for SAS use case

Specific data asset	Impact class for data asset categories		
	Impact class for confidential SHPSF data	**Impact class for integrity relevant SHPSF data**	**Impact class for loss critical availability relevant SHPSF data**
actuator control data for SAS	IMP.CONF.MEDIUM	IMP.INT = Maximum(IMP.FH of controlled actuator control function)	IMP.AVAI.LOSS.MEDIUM
battery status data for SAS	IMP.CONF.LOW	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
cryptographic security parameter for SAS	IMP.CONF = Maximum(Maximum(IMP.CONF, IMP.INT of all data assets whose protection relies on the confidentiality of the cryptographic security parameter),Maximum(IMP.INT, IMP.FH of all function assets whose protection relies on the confidentiality of the cryptographic security parameter))	IMP.INT = Maximum(Maximum(IMP.CONF, IMP.INT of all data assets whose protection relies on the integrity of the cryptographic security parameter),Maximum(IMP.INT, IMP.FH of all function assets whose protection relies on the integrity of the cryptographic security parameter))	IMP.AVAI.LOSS = Maximum(IMP.AVAI.LOSS of all data assets which are lost when the cryptographic security parameter is lost)
device identifier data for SAS	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.LOW
entity's location data for SAS	IMP.CONF.HIGH	IMP.INT.HIGH	IMP.AVAI.LOSS.LOW
function binary data for SAS	NO	IMP.INT = Maximum(IMP.FH, IMP.INT, IMP.AVAI.TIME of function it implements)	NO
function configuration data for SAS	IMP.CONF.MEDIUM	IMP.INT = Maximum(IMP.INT, IMP.AVAI.TIME, IMP.FH of configured function)	IMP.AVAI.LOSS = Maximum(IMP.AVAI.TIME of configured function)
function fault detection data for SAS	IMP.CONF.LOW	IMP.INT.HIGH	IMP.AVAI.LOSS.MEDIUM
health data for SAS	IMP.CONF.HIGH	IMP.INT.HIGH	IMP.AVAI.LOSS.MEDIUM
human emergency detection data for SAS	IMP.CONF.HIGH	IMP.INT.HIGH	IMP.AVAI.LOSS.LOW
logging data for SAS	IMP.CONF = Maximum(IMP.CONF of confidential data contained in the logging data)	IMP.INT = Maximum(IMP.FH of SHPSFs functions using logging data)	IMP.AVAI.LOSS.HIGH
object tamper detection data for SAS	IMP.CONF.MEDIUM	IMP.INT.MEDIUM	IMP.AVAI.LOSS.LOW
other products' function configuration data for SAS	IMP.CONF = Maximum(IMP.FH of other products' configured functions)	IMP.INT = Maximum(IMP.FH, IMP.INT, IMP.AVAI.TIME of other products' configured functions)	IMP.AVAI.LOSS = Maximum(IMP.AVAI.TIME of other products' configured functions)
personal calendar data for SAS	IMP.CONF.HIGH	IMP.INT.HIGH	IMP.AVAI.LOSS.HIGH
personal contact data for SAS	IMP.CONF.HIGH	IMP.INT.HIGH	IMP.AVAI.LOSS.HIGH
personal notes data for SAS	IMP.CONF.HIGH	IMP.INT.HIGH	IMP.AVAI.LOSS.HIGH
private audio data for SAS	IMP.CONF.HIGH	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
private video data for SAS	IMP.CONF.HIGH	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
real-time data for SAS	IMP.CONF.LOW	IMP.INT.MEDIUM	IMP.AVAI.LOSS.MEDIUM
SHPSF tamper detection data for SAS	IMP.CONF.MEDIUM	IMP.INT = Maximum(IMP.INT of architectural component's functions)	IMP.AVAI.LOSS.LOW
state data for SAS	IMP.CONF.MEDIUM	IMP.INT.HIGH	IMP.AVAI.LOSS.MEDIUM

D.2 Function assets

Where no use case specific impact class assignment is provided by the present document, the impact classes shall be assigned to function assets in accordance with tables D.6 and D.7.

Table D.6: Mapping of specific function assets to impact classes for generic 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**
actuator control function	IMP.INT = Maximum(IMP.FH of controlled function)	IMP.AVAI.TIME = Maximum(IMP.AVAI.TIME of controlled function)	IMP.FH = Maximum(IMP.FH.SP, IMP.FH.DSN, IMP.FH.MINT, IMP.FH.CCON of controlled function)
connection function	IMP.INT.LOW	IMP.AVAI.TIME.LOW	IMP.FH.MEDIUM
data communication function	IMP.INT = Maximum(IMP.CONF, IMP.INT of communicated data)	NO	IMP.FH = Maximum(LOW,Maximum(IMP.CONF of communicated data))
data modification function	IMP.INT = Maximum(IMP.INT of modified data)	NO	IMP.FH = Maximum(IMP.INT of modified data)
data presenting function	IMP.INT = Maximum(IMP.CONF, IMP.INT of presented data)	NO	IMP.FH = Maximum(IMP.CONF of presented data)
external sensing function	IMP.INT = Maximum(IMP.INT of measured data)	NO	IMP.FH = Maximum(IMP.CONF, IMP.INT of measured data)
fire/gas alarm function	IMP.INT.MEDIUM	IMP.AVAI.TIME.MEDIUM	IMP.FH.MEDIUM
internal sensing function	IMP.INT = Maximum(IMP.INT of measured data)	NO	IMP.FH = Maximum(IMP.CONF, IMP.INT of measured data)
intrusion and hold up alarm function	IMP.INT.MEDIUM	IMP.AVAI.TIME.MEDIUM	IMP.FH.MEDIUM
other products' configuration function	IMP.INT = Maximum(IMP.INT of other products' configured functions)	IMP.AVAI.TIME = Maximum(IMP.AVAI.TIME of other products' configured functions)	IMP.FH = Maximum(IMP.FH.SP, IMP.FH.DSN, IMP.FH.MINT, IMP.FH.CCON of other products' configured functions)
physical security notification function	IMP.INT.HIGH	IMP.AVAI.TIME.HIGH	IMP.FH.MEDIUM
power supply function	IMP.INT.MEDIUM	IMP.AVAI.TIME = Maximum(IMP.AVAI.TIME of functions of controlled hardware architectural component)	IMP.FH = Maximum(LOW,Maximum(IMP.FH.SP of functions of controlled hardware architectural component))
security function	IMP.INT = Maximum(Maximum(IMP.INT of protected data),Maximum(IMP.INT of protected functions))	IMP.AVAI.TIME = Maximum(IMP.AVAI.TIME of protected functions)	NO

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
SHPSF basic protection object lock function	IMP.INT.LOW	IMP.AVAI.TIME.MEDIUM	IMP.FH.LOW
SHPSF exterior lock function	IMP.INT.MEDIUM	IMP.AVAI.TIME.MEDIUM	IMP.FH.HIGH
SHPSF high protection object lock function	IMP.INT.HIGH	IMP.AVAI.TIME.MEDIUM	IMP.FH.HIGH
SHPSF interior lock function	IMP.INT.MEDIUM	IMP.AVAI.TIME.MEDIUM	IMP.FH.MEDIUM
SHPSF medium protection object lock function	IMP.INT.MEDIUM	IMP.AVAI.TIME.MEDIUM	IMP.FH.MEDIUM
social alarm function	IMP.INT.HIGH	IMP.AVAI.TIME.HIGH	IMP.FH.MEDIUM

The contents of the column *impact class for function whose use can cause harm* of table D.6 are split into details in table D.7.

Table D.7: 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 asset categories			
	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
actuator control function	IMP.FH.SP = Maximum(IMP.FH.SP of controlled function)	IMP.FH.DSN = Maximum(IMP.FH.DSN of controlled function)	IMP.FH.CCON = Maximum(IMP.FH.CCON of controlled function)	IMP.FH.MINT = Maximum(IMP.FH.MINT of controlled function)
connection function	NO	IMP.FH.DSN.MEDIUM	NO	NO
data communication function	NO	IMP.FH.DSN.LOW	IMP.FH.CCON = Maximum(IMP.CONF of communicated data)	NO
data modification function	NO	NO	NO	IMP.FH.MINT = Maximum(IMP.INT of modified data)
data presenting function	IMP.FH.SP = Maximum(IMP.CONF of presented data)	NO	IMP.FH.CCON = Maximum(IMP.CONF of presented data)	NO
external sensing function	IMP.FH.SP = Maximum(IMP.CONF of measured data)	NO	NO	IMP.FH.MINT = Maximum(IMP.INT of measured data)
fire/gas alarm function	IMP.FH.SP.MEDIUM	NO	NO	NO
internal sensing function	IMP.FH.SP = Maximum(IMP.CONF of measured data)	NO	NO	IMP.FH.MINT = Maximum(IMP.INT of measured data)
intrusion and hold up alarm function	IMP.FH.SP.MEDIUM	NO	NO	NO
other products' configuration function	IMP.FH.SP = Maximum(IMP.FH.SP of other products' configured functions)	IMP.FH.DSN = Maximum(IMP.FH.DSN of other products' configured functions)	IMP.FH.CCON = Maximum(IMP.FH.CCON of other products' configured functions)	IMP.FH.MINT = Maximum(IMP.FH.MINT of other products' configured functions)
physical security notification function	IMP.FH.SP.MEDIUM	NO	NO	NO

Specific function asset	Impact class for function asset categories			
	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**
power supply function	IMP.FH.SP = Maximum(IMP.FH.SP of functions of controlled hardware architectural component)	IMP.FH.DSN.LOW	NO	NO
security function	NO	NO	NO	NO
SHPSF basic protection object lock function	IMP.FH.SP.LOW	NO	NO	NO
SHPSF exterior lock function	IMP.FH.SP.HIGH	NO	NO	NO
SHPSF high protection object lock function	IMP.FH.SP.HIGH	NO	NO	NO
SHPSF interior lock function	IMP.FH.SP.MEDIUM	NO	NO	NO
SHPSF medium protection object lock function	IMP.FH.SP.MEDIUM	NO	NO	NO
social alarm function	IMP.FH.SP.MEDIUM	NO	NO	NO

For the specific use cases defined in clause 4.6.2, the corresponding table (tables D.8, D.9, D.10, D.11) shall be used to assign impact classes to function asset.

Table D.8: Mapping of specific function assets to impact classes for generic function asset categories for BIS use case

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**
connection function for BIS	IMP.INT.HIGH	IMP.AVAI.TIME.LOW	IMP.FH.LOW
data communication function for BIS	IMP.INT = Maximum(IMP.CONF, IMP.INT of communicated data)	IMP.AVAI.TIME.HIGH	IMP.FH = Maximum(LOW,Maximum(IMP.CONF of communicated data))
data modification function for BIS	IMP.INT = Maximum(IMP.INT of modified data)	IMP.AVAI.TIME.LOW	IMP.FH = Maximum(HIGH,Maximum(IMP.INT of modified data))
data presenting function for BIS	IMP.INT = Maximum(IMP.CONF, IMP.INT of presented data)	IMP.AVAI.TIME.LOW	IMP.FH = Maximum(IMP.CONF of presented data)
external sensing function for BIS	IMP.INT = Maximum(IMP.INT of measured data)	IMP.AVAI.TIME.HIGH	IMP.FH = Maximum(IMP.CONF, IMP.INT of measured data)
physical security notification function for BIS	IMP.INT.HIGH	IMP.AVAI.TIME.HIGH	IMP.FH.MEDIUM

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**
power supply function for BIS	NO	IMP.AVAI.TIME = Maximum(IMP.AVAI.TIME of functions of controlled hardware architectural component)	IMP.FH = Maximum(IMP.FH.SP of functions of controlled hardware architectural component)
security function for BIS	IMP.INT = Maximum(Maximum(IMP.INT of protected data),Maximum(IMP.INT of protected functions))	IMP.AVAI.TIME = Maximum(IMP.AVAI.TIME of protected functions)	IMP.FH.HIGH
SHPSF exterior lock function for BIS	IMP.INT.MEDIUM	IMP.AVAI.TIME.LOW	IMP.FH.HIGH

Table D.9: Mapping of specific function assets to impact classes for generic function asset categories for FGS use case

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**
actuator control function for FGS	IMP.INT = Maximum(IMP.FH of controlled function)	IMP.AVAI.TIME = Maximum(IMP.AVAI.TIME of controlled function)	IMP.FH = Maximum(IMP.FH.SP, IMP.FH.DSN, IMP.FH.MINT, IMP.FH.CCON of controlled function)
connection function for FGS	IMP.INT.LOW	IMP.AVAI.TIME.LOW	IMP.FH.MEDIUM
data presenting function for FGS	IMP.INT = Maximum(IMP.CONF, IMP.INT of presented data)	IMP.AVAI.TIME.MEDIUM	IMP.FH = Maximum(IMP.CONF of presented data)
fire/gas alarm function for FGS	IMP.INT.MEDIUM	IMP.AVAI.TIME.MEDIUM	IMP.FH.MEDIUM
internal sensing function for FGS	IMP.INT = Maximum(IMP.INT of measured data)	NO	IMP.FH = Maximum(IMP.CONF, IMP.INT of measured data)
other products' configuration function for FGS	IMP.INT = Maximum(IMP.INT of other products' configured functions)	IMP.AVAI.TIME = Maximum(IMP.AVAI.TIME of other products' configured functions)	IMP.FH = Maximum(IMP.FH.SP, IMP.FH.DSN, IMP.FH.MINT, IMP.FH.CCON of other products' configured functions)
physical operational environment sensing function for FGS	IMP.INT = Maximum(IMP.INT of measured data)	NO	IMP.FH = Maximum(IMP.CONF, IMP.INT of measured data)
physical security notification function for FGS	IMP.INT.MEDIUM	IMP.AVAI.TIME.MEDIUM	IMP.FH.MEDIUM
power supply function for FGS	IMP.INT.MEDIUM	IMP.AVAI.TIME = Maximum(IMP.AVAI.TIME of functions of controlled hardware architectural component)	IMP.FH = Maximum(LOW,Maximum(IMP.FH.SP of functions of controlled hardware architectural component))
security function for FGS	IMP.INT = Maximum(Maximum(IMP.INT of protected data),Maximum(IMP.INT of protected functions))	IMP.AVAI.TIME = Maximum(IMP.AVAI.TIME of protected functions)	NO
SHPSF function which can communicate SHPSF data for FGS	IMP.INT = Maximum(IMP.CONF, IMP.INT of communicated data)	IMP.AVAI.TIME.MEDIUM	IMP.FH = Maximum(LOW,Maximum(IMP.CONF of communicated data))
SHPSF function which can modify SHPSF data for FGS	IMP.INT = Maximum(IMP.INT of modified data)	IMP.AVAI.TIME.MEDIUM	IMP.FH = Maximum(IMP.INT of modified data)

Table D.10: Mapping of specific function assets to impact classes for generic function asset categories for I&HAS use case

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**
connection function for I&HAS	IMP.INT.LOW	IMP.AVAI.TIME.LOW	IMP.FH.MEDIUM
data presenting function for I&HAS	IMP.INT = Maximum(IMP.CONF, IMP.INT of presented data)	IMP.AVAI.TIME.MEDIUM	IMP.FH = Maximum(IMP.CONF of presented data)
internal sensing function for I&HAS	IMP.INT = Maximum(IMP.INT of measured data)	IMP.AVAI.TIME.MEDIUM	IMP.FH = Maximum(IMP.CONF, IMP.INT of measured data)
intrusion and hold up alarm function for I&HAS	IMP.INT.MEDIUM	IMP.AVAI.TIME.MEDIUM	IMP.FH.MEDIUM
physical operational environment sensing function for I&HAS	IMP.INT = Maximum(IMP.INT of measured data)	IMP.AVAI.TIME.LOW	IMP.FH = Maximum(IMP.CONF, IMP.INT of measured data)
physical security notification function for I&HAS	IMP.INT.MEDIUM	IMP.AVAI.TIME.MEDIUM	IMP.FH.MEDIUM
power supply function for I&HAS	IMP.INT.MEDIUM	IMP.AVAI.TIME = Maximum(IMP.AVAI.TIME of functions of controlled hardware architectural component)	IMP.FH = Maximum(MEDIUM,Maximum(IMP.FH.SP of functions of controlled hardware architectural component))
security function for I&HAS	IMP.INT = Maximum(Maximum(IMP.INT of protected data),Maximum(IMP.INT of protected functions))	IMP.AVAI.TIME = Maximum(IMP.AVAI.TIME of protected functions)	NO
SHPSF function which can communicate SHPSF data for I&HAS	IMP.INT = Maximum(IMP.CONF, IMP.INT of communicated data)	NO	IMP.FH = Maximum(LOW,Maximum(IMP.CONF of communicated data))
SHPSF function which can modify SHPSF data for I&HAS	IMP.INT = Maximum(IMP.INT of modified data)	NO	IMP.FH = Maximum(IMP.INT of modified data)

Table D.11: Mapping of specific function assets to impact classes for generic function asset categories for SAS use case

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**
connection function for SAS	IMP.INT.LOW	IMP.AVAI.TIME.LOW	IMP.FH.MEDIUM
data presenting function for SAS	IMP.INT = Maximum(IMP.CONF, IMP.INT of presented data)	NO	IMP.FH = Maximum(IMP.CONF of presented data)
internal sensing function for SAS	IMP.INT = Maximum(IMP.INT of measured data)	NO	IMP.FH = Maximum(IMP.CONF, IMP.INT of measured data)
other products' configuration function for SAS	IMP.INT = Maximum(IMP.INT of other products' configured functions)	IMP.AVAI.TIME = Maximum(IMP.AVAI.TIME of other products' configured functions)	IMP.FH = Maximum(IMP.FH.SP, IMP.FH.DSN, IMP.FH.MINT, IMP.FH.CCON of other products' configured functions)
physical operational environment sensing function for SAS	IMP.INT = Maximum(IMP.INT of measured data)	IMP.AVAI.TIME.HIGH	IMP.FH = Maximum(IMP.CONF, IMP.INT of measured data)
physical security notification function for SAS	IMP.INT.HIGH	IMP.AVAI.TIME.HIGH	IMP.FH.MEDIUM
power supply function for SAS	IMP.INT.MEDIUM	IMP.AVAI.TIME = Maximum(IMP.AVAI.TIME of functions of controlled hardware architectural component)	IMP.FH = Maximum(LOW,Maximum(IMP.FH.SP of functions of controlled hardware architectural component))
security function for SAS	IMP.INT = Maximum(Maximum(IMP.INT of protected data),Maximum(IMP.INT of protected functions))	IMP.AVAI.TIME = Maximum(IMP.AVAI.TIME of protected functions)	NO
SHPSF function which can communicate SHPSF data for SAS	IMP.INT = Maximum(IMP.CONF, IMP.INT of communicated data)	NO	IMP.FH = Maximum(LOW,Maximum(IMP.CONF of communicated data))
SHPSF function which can modify SHPSF data for SAS	IMP.INT = Maximum(IMP.INT of modified data)	NO	IMP.FH = Maximum(IMP.INT of modified data)
social alarm function for SAS	IMP.INT.HIGH	IMP.AVAI.TIME.HIGH	IMP.FH.HIGH

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.Normal, 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 (V1.1.1) [i.8].

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 cryptographic parameter guessing probability 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-Normal] AUTH.Normal inherence based SFA

Where an authentication factor of the type inherence is used to achieve AUTH.Normal, 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 (V1.1.1) [i.8].

E.1.1.5 [AUM-E-K-Normal] AUTH.Normal 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 month ($2{,}6 \times 10^{6}$ seconds) with a cryptographic parameter guessing probability 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-Normal] AUTH.Normal possession based SFA

Where an Account or Service is used as an possession type authentication factor to achieve AUTH.Normal, 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 that can be valid at the same time have a combined cryptographic parameter guessing probability 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 800-78-5 [i.9].

E.1.1.7 [AUM-E-MFA-Normal] AUTH.Normal MFA

Where multiple authentication factors are used to achieve AUTH.Normal, 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.Basic, the authentication mechanisms shall ensure a false acceptance rate of maximal 5×10^{-5} and a false rejection rate of maximal 3×10^{-2}.

NOTE: The values used for false acceptance rate and false rejection rate are based on ETSI TS 103 732-2 (V1.1.1) [i.8].

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.Normal, the authentication mechanisms shall ensure a security insurance time of one year ($3{,}2 \times 10^{7}$ seconds) with a cryptographic parameter guessing probability 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 an possession type authentication factor to achieve AUTH.Enhanced, the authentication mechanisms shall ensure that:

- confidential cryptographic keys in security tokens have a 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 that can be valid at the same time have a combined cryptographic parameter guessing probability 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 800-78-5 [i.9].

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.Normal 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 3×10^{-2}.

NOTE: The values used for false acceptance rate and false rejection rate are based on ETSI TS 103 732-2 (V1.1.1) [i.8].

E.1.1.13 [AUM-E-P-Strong] AUTH.Strong possession based SFA

Where a security token is used as an 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 a 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 that can be valid at the same time have a combined cryptographic parameter guessing probability 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 800-78-5 [i.9].

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.Normal, 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.Normal, 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 SHPSF and another entity.

E.1.1.16 [AUM-E-PitM] AUTH.Normal, 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.Normal, 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 SHPSF 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 reference:

[AUM-E-I-Basic]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the SHPSF 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.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the authentication mechanism used by the SHPSF 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; and
- 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; and
- determine the FAR value of the authentication mechanism; and
- 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 reference:

[AUM-E-K-Basic]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the SHPSF 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.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the authentication mechanism used by the SHPSF 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; and
- 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; and
- determine the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) value of the authentication mechanism; and
- determine the maximum sustained validation attempt frequency ($f_{VA,max}$) value of the authentication mechanism; and
- calculate the cryptographic parameter guessing probability (p_{GRP}) for a security insurance time (security insurance time) of one day $p_{GRP} = T_{SI} * f_{VA,max} / C_{CP,min}$.

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-Normal]

Assessment reference:

[AUM-E-I-Normal]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the SHPSF to fulfil [AUM-FH] clause 5.6.2 for authentication level AUTH.Normal using inherence authentication factors,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the authentication mechanism used by the SHPSF to achieve AUTH.Normal 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.Normal is created; and
- 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; and
- determine the FAR value of the authentication mechanism; and
- determine the FRR value of the authentication mechanism.

Assessment verdict:

The verdict PASS shall be assigned if:

- the authentication mechanism used to achieve AUTH.Normal with inherence authentication factors has a FAR of maximal 5×10^{-5}; and
- the authentication mechanism used to achieve AUTH.Normal with inherence authentication factors has a FRR of maximal 10^{-1}; and
- there is no indication, that an authentication mechanisms used to achieve AUTH.Normal 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-Normal]

Assessment reference:

[AUM-E-K-Normal]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the SHPSF to fulfil [AUM-FH] clause 5.6.2 for authentication level AUTH.Normal using knowledge authentication factors,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the authentication mechanism used by the SHPSF to achieve AUTH.Normal 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.Normal is created; and
- 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; and
- determine the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) value of the authentication mechanism; and
- determine the maximum sustained validation attempt frequency ($f_{VA,max}$) value of the authentication mechanism; and
- calculate the cryptographic parameter guessing probability (p_{GRP}) for a security insurance time (T_{SI}) of one month ($2{,}6 \times 10^6$ seconds) $p_{GRP} = T_{SI} * f_{VA,max} / C_{CP,min}$.

Assessment verdict:

The verdict PASS shall be assigned if:

- the authentication mechanism used to achieve AUTH.Normal 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.Normal 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-Normal]

Assessment reference:

[AUM-E-P-Normal]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the SHPSF to fulfil [AUM-FH] clause 5.6.2 for authentication level AUTH.Normal using possession authentication factors based on Accounts or Services

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the authentication mechanism used by the SHPSF to achieve AUTH.Normal using possession authentication factors based on Accounts or Services:
  - documentation of Accounts or Services that can be used by the authentication mechanism; and
  - 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.Normal is created; and
- a suitable security token is known to the authentication mechanism; and
- 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; and
- 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; and
  - determine the maximal valid derived tokens ($n_{dt,max}$); and
  - determine the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) value of the authentication mechanism; and
  - determine the maximum sustained validation attempt frequency ($f_{VA,max}$) value of the authentication mechanism; and
  - calculate the combined cryptographic parameter guessing probability (p_{GRP}) for the derived tokens, that can be valid at the same time: $p_{GRP} = T_{VA} * f_{VA,max} * n_{dt,max} / C_{CP,min}$.

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 cryptographic parameter guessing probability of maximal 10^{-3}; and
- there is no indication, that the authentication mechanisms used to achieve AUTH.Normal 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-Normal]

Assessment reference:

[AUM-E-MFA-Normal]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the SHPSF to fulfil [AUM-FH] clause 5.6.2 for authentication level AUTH.Normal using MFA,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the authentication mechanism used by the SHPSF to achieve AUTH.Normal 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.Normal is created; and
- 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; and
- verify whether authentication factors of the same type can be used for MFA; and
- 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); and
- 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.1.2.2); and
- for authentication factors based on possession, verify whether the authentication mechanism would satisfy the assessment clause E.1.2.6 (or clause E.1.2.0, clause E.1.2.3); and
- 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.Normal 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.Normal 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 reference:

[AUM-E-I-Enhanced]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the SHPSF 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.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the authentication mechanism used by the SHPSF 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; and
- 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; and
- determine the FAR value of the authentication mechanism; and
- 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 5×10^{-5}; and
- the authentication mechanism used to achieve AUTH.Enhanced with inherence authentication factors has a FRR of maximal 3×10^{-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 reference:

[AUM-E-K-Enhanced]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the SHPSF 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.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the authentication mechanism used by the SHPSF 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; and
- 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; and
- determine the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) value of the authentication mechanism; and
- determine the maximum sustained validation attempt frequency ($f_{VA,max}$) value of the authentication mechanism; and
- calculate the cryptographic parameter guessing probability (p_{GRP}) for a security insurance time (T_{SI}) of one year ($3{,}2 \times 10^7$ seconds) $p_{GRP} = T_{SI} * f_{VA,max} / C_{CP,min}$.

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 reference:

[AUM-E-P-Enhanced] for accounts or services used as an authentication factor

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the SHPSF 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.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the authentication mechanism used by the SHPSF 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; and
  - 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; and
- a suitable security token is known to the authentication mechanism; and
- 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; and
- 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; and
  - determine the maximal valid derived tokens ($n_{dt,max}$); and
  - determine the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) value of the authentication mechanism; and
  - determine the maximum sustained validation attempt frequency ($f_{VA,max}$) value of the authentication mechanism; and
  - calculate the combined cryptographic parameter guessing probability (p_{GRP}) for the derived tokens, that can be valid at the same time: $p_{GRP} = T_{VA} * f_{VA,max} * n_{dt,max} / C_{CP,min}$.

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 cryptographic parameter guessing probability 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 reference:

[AUM-E-P-Enhanced] for a security token used as an authentication factor

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the SHPSF 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.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the authentication mechanism used by the SHPSF 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; and
- suitable security tokens for the documented authentication mechanisms; and
- 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; and
- determine the minimal effective cryptographic security parameter bitlength of the security tokens that can be used by the authentication mechanism; and
- 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; and
  - determine the maximal valid derived tokens ($n_{dt,max}$); and
  - determine the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) value of the derived tokens; and
  - determine the maximum sustained validation attempt frequency ($f_{VA,max}$) value of the authentication mechanism; and
  - calculate the combined cryptographic parameter guessing probability (p_{GRP}) for the derived tokens, that can be valid at the same time: $p_{GRP} = T_{VA} * f_{VA,max} * n_{dt,max} / C_{CP,min}$.

Assessment verdict:

The verdict PASS shall be assigned if:

- security tokens have a 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 cryptographic parameter guessing probability 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 reference:

[AUM-E-MFA-Enhanced]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the SHPSF 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.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the authentication mechanism used by the SHPSF 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; and
- 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; and
- verify whether authentication factors of the same type can be used for MFA; and
- 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); and
- 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.1.2.2); and
- for authentication factors based on possession, verify whether the authentication mechanism would satisfy the assessment clause E.1.2.6 (or clause E.1.2.0, clause E.1.2.3); and

- 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.Normal 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 reference:

[AUM-E-I-Strong]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the SHPSF 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.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the authentication mechanism used by the SHPSF 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; and
- 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; and
- determine the FAR value of the authentication mechanism; and
- 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 3×10^{-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 reference:

[AUM-E-P-Strong]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the SHPSF 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.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the authentication mechanism used by the SHPSF 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; and
- suitable security tokens for the documented authentication mechanisms; and
- 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; and
- determine the minimal effective cryptographic security parameter bitlength of the security tokens that can be used by the authentication mechanism; and
- 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; and

- determine the maximal valid derived tokens ($n_{dt,max}$); and
- determine the minimal recommended cryptographic security parameter complexity ($C_{CP,min}$) value of the derived tokens; and
- determine the maximum sustained validation attempt frequency ($f_{VA,max}$) value of the authentication mechanism; and
- calculate the combined cryptographic parameter guessing probability (p_{GRP}) for the derived tokens, that can be valid at the same time: $p_{GRP} = T_{VA} * f_{VA,max} * n_{dt,max} / C_{CP,min}$.

Assessment verdict:

The verdict PASS shall be assigned if:

- security tokens have a 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 cryptographic parameter guessing probability 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 reference:

[AUM-E-MFA-Strong]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an authentication mechanism used by the SHPSF 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.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the authentication mechanism used by the SHPSF 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; and
- 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; and
- verify whether authentication factors of the same type can be used for MFA; and

- for authentication factors based on knowledge, verify whether the authentication mechanism would satisfy the assessment clause E.1.2.9; and
- for authentication factors based on inherence, verify whether the authentication mechanism would satisfy the assessment clause E.1.2.8 (or clause E.1.2.2); and
- for authentication factors based on possession, verify whether the authentication mechanism would satisfy the assessment clause E.1.2.0 (or clause E.1.2.3); and
- 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.Normal 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 reference:

[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.Normal, AUTH.Enhanced or AUTH.Strong,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the authentication mechanism that are accessible via interfaces with local communication, adjacent communication or public communication and provide AUTH.Normal, 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 SHPSF; and
- a capture and replay tool between SHPSF and its communication partner shall be set up; and
- at least one interface, where the authentication mechanism is reachable shall be documented.

Assessment activities:

The following activities shall be performed:

- for authentication mechanisms that are accessible via interfaces with local communication, adjacent communication or public communication and provide AUTH.Normal, AUTH.Enhanced or AUTH.Strong:
  - initiate a connection between the SHPSF and its communication partner; and
  - use a capture tool to record the transmitted message or transaction data; and
  - replay (retransmit) the captured message to the authentication mechanism using a suitable tool in place to mimic the original communication partner; and
  - 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 reference:

[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.Normal, AUTH.Enhanced or AUTH.Strong,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the authentication mechanism that are accessible via interfaces with local communication, adjacent communication or public communication and provide AUTH.Normal, 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 SHPSF; and
- a capture and PitM tool between SHPSF and its communication partner shall be set up; and
- at least one interface, where the authentication mechanism is reachable shall be documented.

Assessment activities:

The following activities shall be performed:

- for authentication mechanisms that are accessible via interfaces with local communication, adjacent communication or public communication and provide AUTH.Normal, AUTH.Enhanced or AUTH.Strong:
  - initiate a connection between the SHPSF and its communication partner; and
  - 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; and
  - 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-Normal] INT.SSM.Normal integrity protecting secure storage mechanism

Where an integrity protecting secure storage mechanism is used to achieve INT.SSM.Normal, 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 authorised 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 authorised user is authenticated and - the confidential cryptographic key is protected against unauthorised 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 reference:

[INT-SSM-E-Basic]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an integrity protecting secure storage mechanism used by the SHPSF to fulfil [INT-SSM] clause 5.8.1 for authentication level INT.SSM.Basic,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the integrity protecting secure storage mechanism used by the SHPSF 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-Normal]

Assessment reference:

[INT-SSM-E-Normal]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an integrity protecting secure storage mechanism used by the SHPSF to fulfil [INT-SSM] clause 5.8.1 for authentication level INT.SSM.Basic,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the integrity protecting secure storage mechanism used by the SHPSF 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; and
- verify whether stored integrity relevant data is not targeted modifiable until an authorised 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 authorised 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 reference:

[INT-SSM-E-Enhanced]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an integrity protecting secure storage mechanism used by the SHPSF to fulfil [INT-SSM] clause 5.8.1 for authentication level INT.SSM.Enhanced,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the integrity protecting secure storage mechanism used by the SHPSF 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; and
- verify whether stored integrity relevant data is not targeted modifiable until an authorised user is authenticated; and

- verify whether confidential cryptographic keys used to protect against targeted modification of stored data is protected against unauthorised 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 authorised user is authenticated; and
- the confidential cryptographic keys used to protect against targeted modification of stored data is protected against unauthorised 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 reference:

[INT-SSM-E-Strong]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an integrity protecting secure storage mechanism used by the SHPSF to fulfil [INT-SSM] clause 5.8.1 for authentication level INT.SSM.Strong,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the integrity protecting secure storage mechanism used by the SHPSF 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 5.8.2. Note that for CONF.COM.Normal, 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.10], IETF RFC 8613 [i.11], IETF RFC 9528 [i.12] and IETF RFC 9147 [i.13].

E.2.3.3 [INT-COM-E-Normal] INT.COM.Normal 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 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 integrity of communicated integrity relevant data.

NOTE: The values used for effective cryptographic security parameter bitlength are based on IETF RFC 8446 [i.10], IETF RFC 8613 [i.11], IETF RFC 9528 [i.12] and IETF RFC 9147 [i.13].

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 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 integrity of communicated integrity relevant data.

NOTE: The values used for effective cryptographic security parameter bitlength are based on IETF RFC 8446 [i.10], IETF RFC 8613 [i.11], IETF RFC 9528 [i.12] and IETF RFC 9147 [i.13].

E.2.3.5 [INT-COM-E-EndAuth] INT.COM.Normal and INT.COM.Enhanced integrity protecting communication mechanism endpoint authentification

Where an integrity protecting communication mechanism is used to achieve INT.COM.Normal 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.Normal and INT.COM.Enhanced integrity protecting communication mechanism downgrade protection

Where an integrity protecting communication mechanism is used to achieve INT.COM.Normal 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 5.8.2.

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 5.8.2.

E.2.4.2 Assessment criteria for [INT-COM-E-Basic]

Assessment reference:

[INT-COM-E-Basic]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an integrity protecting communication mechanism used by the SHPSF to fulfil [INT-COM] clause 5.8.2 for authentication level INT.COM.Basic,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the integrity protecting communication mechanism used by the SHPSF 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; and

- 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-Normal]

Assessment reference:

[INT-COM-E-Normal]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an integrity protecting communication mechanism used by the SHPSF to fulfil [INT-COM] clause 5.8.2 for authentication level INT.COM.Normal,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the integrity protecting communication mechanism used by the SHPSF to achieve INT.COM.Normal:
  - documentation of the confidential cryptographic keys used to protect the integrity of communicated integrity relevant data; and
  - 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; and
- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect the integrity of communicated integrity relevant data; and

- 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; and
  - determine the amount of data that can be communicated during this time.

Assessment verdict:

The verdict PASS shall be assigned if:

- there is no indication, that the integrity protecting communication mechanism used to achieve INT.COM.Normal differs from the documentation; and
  - the integrity protecting communication mechanism used to achieve INT.COM.Normal 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 1 GB of data, only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit.

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 reference:

[INT-COM-E-Enhanced]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an integrity protecting communication mechanism used by the SHPSF to fulfil [INT-COM] clause 5.8.2 for authentication level INT.COM.Enhanced,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the integrity protecting communication mechanism used by the SHPSF to achieve INT.COM.Enhanced:
  - documentation of the confidential cryptographic keys used to protect the integrity of communicated integrity relevant data; and
  - 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; and
- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect the integrity of communicated integrity relevant data; and
- 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; and
  - determine the amount of data that can be communicated during this time.

Assessment verdict:

The verdict PASS shall be assigned if:

- there is no indication, that the integrity protecting communication mechanism used to achieve INT.COM.Enhanced differs from the documentation; and
  - 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 1 GB of data, only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit.

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 reference:

[INT-COM-E-EndAuth]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an integrity protecting communication mechanism used by the SHPSF to fulfil [INT-COM] clause 5.8.2 for authentication level INT.COM.Normal or INT.COM.Enhanced,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the integrity protecting communication mechanism used by the SHPSF to achieve INT.COM.Normal 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; and
- 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 reference:

[INT-COM-E-Downgrade]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an integrity protecting communication mechanism used by the SHPSF to fulfil [INT-COM] clause 5.8.2 for authentication level INT.COM.Normal or INT.COM.Enhanced,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the integrity protecting communication mechanism used by the SHPSF to achieve INT.COM.Normal 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; and
- 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.Normal or INT.COM.Enhanced respectively; and
- verify whether the integrity protecting communication mechanism refuses alteration of communication protocol parameters that would result in a protection level below INT.COM.Normal 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.Normal 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.Normal 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

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

E.2.5.2 [INT-SWPCK-E-Basic] INT.SW.VER.Basic software package verification mechanism

Where an software package verification mechanism is used to achieve INT.SW.VER.Basic, the software package verification mechanism shall:

- explicitly obtain the confirmation of an authorised 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 authorised 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-Normal] INT.SW.VER.Normal software package verification mechanism

Where an software package verification mechanism is used to achieve INT.SW.VER.Normal, 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 an 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 5.8.3.

E.2.6.2 Assessment criteria for [INT-SWPCK-E-Basic]

Assessment reference:

[INT-SWPCK-E-Basic]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an software package verification mechanism used by the SHPSF to fulfil [INT-SWPCK] clause 5.8.3 for authentication level INT.SW.VER.Basic,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the software package verification mechanism used by the SHPSF to achieve INT.SW.VER.Basic:
  - documentation of the measures to confirm, that the integrity and authenticity 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; and
- a software package to perform a software update; and
- 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 authorised identity that the integrity and authenticity of a software package has been verified by the authorised identity is explicitly obtained by the software package verification mechanism used to achieve INT.SW.VER.Basic

or

- verify whether the confirmation of an authorised identity that the authenticity of a software package has been verified by the authorised identity is explicitly obtained by the software package verification mechanism used to achieve INT.SW.VER.Basic; and

- verify whether an authorised identity is provided with a hash or checksum to verify the integrity 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:

- there is no indication, that by the software package verification mechanism used to achieve INT.SW.VER.Basic differs from the documentation;

and

- either, the confirmation of an authorised identity that the integrity and authenticity of a software package has been verified by the authorised identity is explicitly obtained by the software package verification mechanism used to achieve INT.SW.VER.Basic; or
  - the confirmation of an authorised identity that the authenticity of a software package has been verified by the authorised identity is explicitly obtained by the software package verification mechanism used to achieve INT.SW.VER.Basic; and
  - an authorised identity is provided with a hash or checksum to verify the integrity of a software package by the software package verification mechanism used to achieve INT.SW.VER.Basic.

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-Normal]

Assessment reference:

[INT-SWPCK-E-Normal]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an software package verification mechanism used by the SHPSF to fulfil [INT-SWPCK] clause 5.8.3 for authentication level INT.SW.VER.Normal.

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the software package verification mechanism used by the SHPSF to achieve INT.SW.VER.Normal:
  - documentation of the measures to ensure that a software package has been obtained from a trusted source over a secure communication channel; and:
    - 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; and
- a communication connection to a trusted source of software packages to perform a software update; and
- 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; and
- 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.Normal 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 reference:

[INT-SWPCK-E-Enhanced]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an software package verification mechanism used by the SHPSF to fulfil [INT-SWPCK] clause 5.8.3 for authentication level INT.SW.VER.Enhanced,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the software package verification mechanism used by the SHPSF to achieve INT.SW.VER.Enhanced:
  - documentation of the measures to verify the integrity and authenticity of a software package using cryptographic digital signatures; and
  - documentation of the cryptographic digital signatures used to verify the integrity and authenticity 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; and
- software packages to perform a software update; and
- 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 integrity and authenticity of a software package using cryptographic digital signatures; and
- determine the $L_{CP,eff}$ of the cryptographic digital signatures used to verify the integrity and authenticity of a software package.

Assessment verdict:

The verdict PASS shall be assigned if:

- the software package verification mechanism verifies the integrity and authenticity of a software package using cryptographic digital signatures; and
- the cryptographic digital signatures used to verify the integrity and authenticity 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 an 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.10], IETF RFC 8613 [i.11], IETF RFC 9528 [i.12] and IETF RFC 9147 [i.13].

E.3.1.3 [CONF-SSM-E-Normal] CONF.SSM.Normal confidentiality protecting secure storage mechanism

Where an confidentiality protecting secure storage mechanism is used to achieve CONF.SSM.Normal, 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 authorised user is authenticated.

NOTE: The values used for effective cryptographic security parameter bitlength are based on IETF RFC 8446 [i.10], IETF RFC 8613 [i.11], IETF RFC 9528 [i.12] and IETF RFC 9147 [i.13].

E.3.1.4 [CONF-SSM-E-Enhanced] CONF.SSM.Enhanced confidentiality protecting secure storage mechanism

Where an 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 authorised user is authenticated and - the confidential cryptographic key is protected against unauthorised access by hardware measures.

NOTE: The values used for effective cryptographic security parameter bitlength are based on IETF RFC 8446 [i.10], IETF RFC 8613 [i.11], IETF RFC 9528 [i.12] and IETF RFC 9147 [i.13].

E.3.1.5 [CONF-SSM-E-Strong] CONF.SSM.Strong confidentiality protecting secure storage mechanism

Where an 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 integrity 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 reference:

[CONF-SSM-E-Basic]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an confidentiality protecting secure storage mechanism used by the SHPSF to fulfil [CONF-SSM] clause 5.7.1 for authentication level CONF.SSM.Normal,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the confidentiality protecting secure storage mechanism used by the SHPSF to achieve CONF.SSM.Normal:
  - 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.Normal 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.Normal 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-Normal]

Assessment reference:

[CONF-SSM-E-Normal]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an confidentiality protecting secure storage mechanism used by the SHPSF to fulfil [CONF-SSM] clause 5.7.1 for authentication level CONF.SSM.Basic,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the confidentiality protecting secure storage mechanism used by the SHPSF 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; and
- verify whether stored confidential data is not readably in plain text until an authorised 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 authorised 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 reference:

[CONF-SSM-E-Enhanced]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an confidentiality protecting secure storage mechanism used by the SHPSF to fulfil [CONF-SSM] clause 5.7.1 for authentication level CONF.SSM.Enhanced,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the confidentiality protecting secure storage mechanism used by the SHPSF 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; and
- verify whether stored confidential data is not readably in plain text until an authorised user is authenticated; and
- verify whether confidential cryptographic keys used to protect the confidentiality of stored confidential data is protected against unauthorised 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 authorised user is authenticated; and
- the confidential cryptographic keys used to protect the confidentiality of stored confidential data is protected against unauthorised 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 reference:

[CONF-SSM-E-Strong]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an confidentiality protecting secure storage mechanism used by the SHPSF to fulfil [CONF-SSM] clause 5.7.1 for authentication level CONF.SSM.Strong,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the confidentiality protecting secure storage mechanism used by the SHPSF 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.Normal, 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 an 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.10], IETF RFC 8613 [i.11], IETF RFC 9528 [i.12] and IETF RFC 9147 [i.13].

E.3.3.3 [CONF-COM-E-Normal] CONF.COM.Normal confidentiality protecting communication mechanism

Where an 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.10], IETF RFC 8613 [i.11], IETF RFC 9528 [i.12] and IETF RFC 9147 [i.13].

E.3.3.4 [CONF-COM-E-Enhanced] CONF.COM.Enhanced confidentiality protecting communication mechanism

Where an 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.10], IETF RFC 8613 [i.11], IETF RFC 9528 [i.12] and IETF RFC 9147 [i.13].

E.3.3.5 [CONF-COM-E-EndAuth] CONF.COM.Normal and CONF.COM.Enhanced confidentiality protecting communication mechanism endpoint authentification

Where an confidentiality protecting communication mechanism is used to achieve CONF.COM.Normal 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.Normal and CONF.COM.Enhanced confidentiality protecting communication mechanism downgrade protection

Where an confidentiality protecting communication mechanism is used to achieve CONF.COM.Normal 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 5.8.2.

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 reference:

[CONF-COM-E-Basic]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an confidentiality protecting communication mechanism used by the SHPSF to fulfil [CONF-COM] clause 5.7.2 for authentication level CONF.COM.Basic,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the confidentiality protecting communication mechanism used by the SHPSF 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; and
- 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-Normal]

Assessment reference:

[CONF-COM-E-Normal]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an confidentiality protecting communication mechanism used by the SHPSF to fulfil [CONF-COM] clause 5.7.2 for authentication level CONF.COM.Normal,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the confidentiality protecting communication mechanism used by the SHPSF to achieve CONF.COM.Normal:
  - documentation of the confidential cryptographic keys used to protect the confidentiality of communicated confidential data; and
  - 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; and
- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect the confidentiality of communicated confidential data; and
  - 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; and
    - determine the amount of data that can be communicated during this time.

Assessment verdict:

The verdict PASS shall be assigned if:

- there is no indication, that the confidentiality protecting communication mechanism used to achieve CONF.COM.Normal differs from the documentation; and
  - the confidentiality protecting communication mechanism used to achieve CONF.COM.Normal 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 1 GB of data, only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit.

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 reference:

[CONF-COM-E-Enhanced]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an confidentiality protecting communication mechanism used by the SHPSF to fulfil [CONF-COM] clause 5.7.2 for authentication level CONF.COM.Enhanced,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the confidentiality protecting communication mechanism used by the SHPSF to achieve CONF.COM.Enhanced:
  - documentation of the confidential cryptographic keys used to protect the confidentiality of communicated confidential data; and
  - 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; and
- determine the $L_{CP,eff}$ value of the confidential cryptographic keys used to protect the confidentiality of communicated confidential data; and
- 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; and
  - determine the amount of data that can be communicated during this time.

Assessment verdict:

The verdict PASS shall be assigned if:

- there is no indication, that the confidentiality protecting communication mechanism used to achieve CONF.COM.Enhanced differs from the documentation; and
  - 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 1 GB of data, only confidential cryptographic keys with a $L_{CP,eff}$ of minimal 112 bit.

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 reference:

[CONF-COM-E-EndAuth]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an confidentiality protecting communication mechanism used by the SHPSF to fulfil [CONF-COM] clause 5.7.2 for authentication level CONF.COM.Normal or CONF.COM.Enhanced,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the confidentiality protecting communication mechanism used by the SHPSF to achieve CONF.COM.Normal 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; and
- 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 reference:

[CONF-COM-E-Downgrade]

Assessment objective:

The assessment covers:

- a functional sufficiency assessment of an confidentiality protecting communication mechanism used by the SHPSF to fulfil [CONF-COM] clause 5.7.2 for authentication level CONF.COM.Normal or CONF.COM.Enhanced,

based on the default configuration required by clause 5.4.

Assessment preparation:

The following documentation for the SHPSF shall be complete:

- for the confidentiality protecting communication mechanism used by the SHPSF to achieve CONF.COM.Normal 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; and
- 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.Normal or CONF.COM.Enhanced respectively; and
- verify whether the confidentiality protecting communication mechanism refuses alteration of communication protocol parameters that would result in a protection level below CONF.COM.Normal 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.Normal 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.Normal 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 "17." by Commission Implementing 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 "17." by Commission Implementing 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. Such cases should be notified to ETSI at the following e-mail address: cybersupport@etsi.org to consider 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 clause 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 3: 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 SHPSFs configuration are different whether the changes can be made via a web GUI, accessible from adjacent or public networks, a GUI, accessible from the SHPSFs touchscreen, or a console, accessible be connecting to a serial port. All of these cases can be simultaneously present on the same SHPSF.

- 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 clause 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 assessment evidences for the assessment.

Figure F.1 provides a graphical representation of the guidance for the application of the present document.

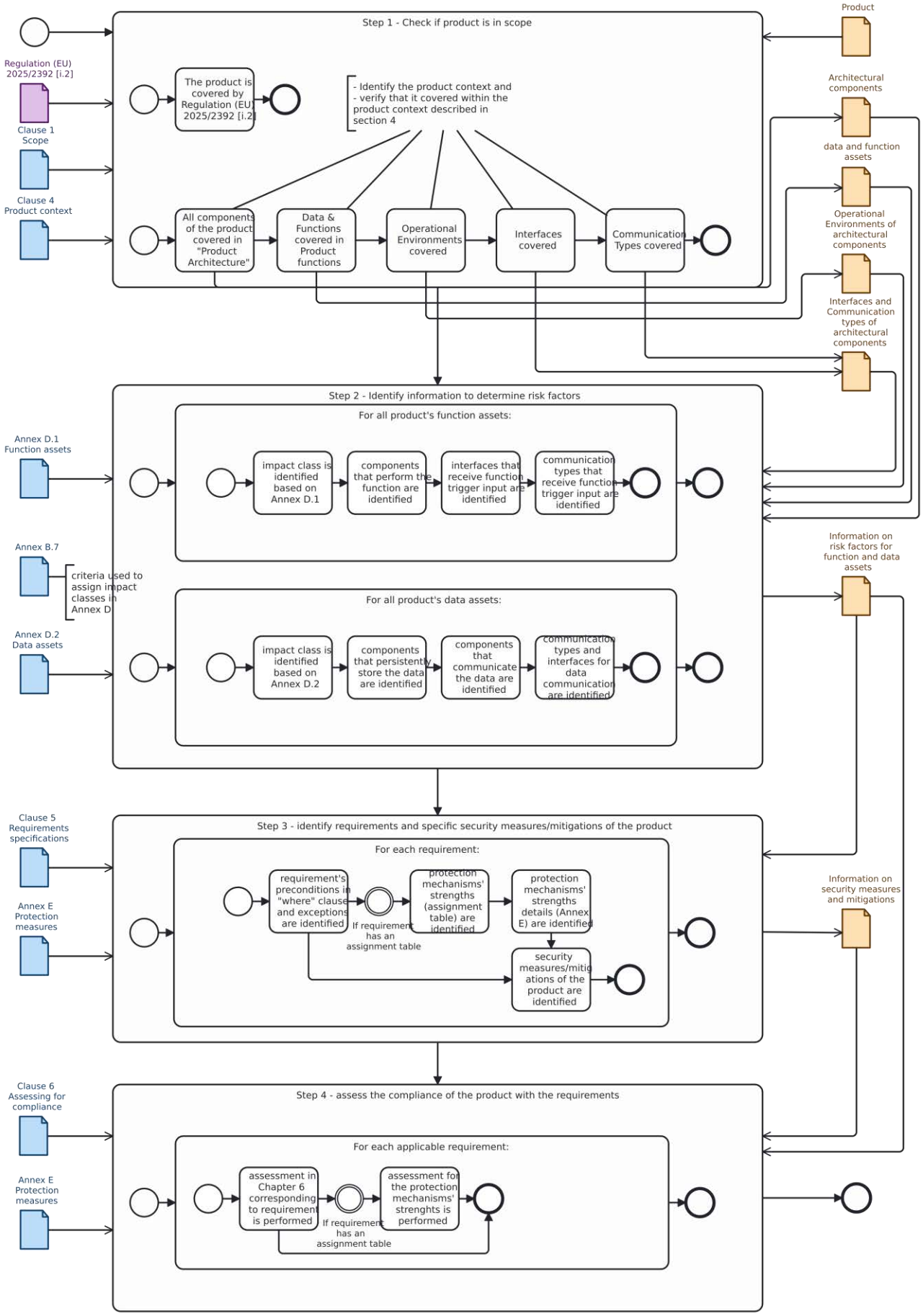

Figure F.1: Graphical representation on guidance for the application of the present document

Annex G: Void

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

H.1 General

The specific use-cases defined the present document use specific terminology in their own context for the data assets and the function assets. This informative annex provides a mapping of the terminology in the context other existing standards related to the specific use-cases with the data assets and function assets defined and used in the present document. The intention is to help readers familiar with the corresponding terminology with the application of this standard for products belonging to those specific use-cases.

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

The terminology mappings for BISs based on EN IEC 62820 series (IEC 62820-1-1:2026 [i.14], IEC 62820-1-2 :2017 [i.15], IEC 62820-2:2017 [i.16], IEC 62820-3-1:2017 [i.17] and IEC 62820-3-2:2018 [i.18]) of standards are provided in tables H.1 and H.2.

Table H.1: Mapping of BIS specific data assets to data assets

BIS specific data assets	Data assets
authentication credentials	cryptographic security parameter or identity data for authentication
authorised users identifiers	identity data for authentication
command of a door lock	actuator control data
communicated multimedia data streams (conversation between VCU or URU and smart device)	private audio data and/or private video data
communicated multimedia data streams (video stream between VCU and smart device)	private video data
communication signalling	function configuration data
conversation state	state data
door status	window/door opening status data
logged event	logging data
name of resident (remote management)	personal contact data
name of service user	personal contact data
real time clock data	real-time data
site specific configuration	function configuration data
site/device identifier	device identifier data
source location identifier (e.g. GPS or Cellular positioning)	entity's location data and identity data for authentication
system configuration	function configuration data
tamper detection data (VCU or URU unmounted from its place)	SHPSF tamper detection data
the time of a logged event	real-time data and logging data
time stamp on recorded photo or video	real-time data and private video data

Table H.2: Mapping of BIS specific function assets to function assets

BIS specific function assets	Function assets
call function	data communication function
communication triggering function	connection function
configuration function	data modification function
door left open or door forced detection function	external sensing function
door lock control function	SHPSF exterior lock function
interconnection function	connection function
localisation function	external sensing function
logging function	data modification function and potentially data communication function
multimedia input function	external sensing function or data communication function
multimedia output function	data presenting function or data communication function
power supply function	power supply function
real time clock	external sensing function
tamper detection function	external sensing function
user access control function	security function
user interface function	data presenting function

H.3 Terminology mappings for fire/gas detection device/systems (FGS)

The terminology mappings for FGSs based on EN 14604 [i.19], BS 5446-2:2003 [i.20], EN 50291-1 [i.21] and EN 50194-1 [i.22] are provided in tables H.3 and H.4.

Table H.3: Mapping of FGS specific data assets to data assets

FGS specific data assets	Data assets
actuator control data (ventilation or other ancillary device)	actuator control data or other products' function configuration data
alarm state of a zone	state data or fire detection data or inflammable/explosive gas detection data
authentication credentials	cryptographic security parameter or identity data for authentication
authorised users identifiers	identity data for authentication
fault detection data	function fault detection data
fault state of a zone	state data or function fault detection data
logged event	logging data
measured physical parameter related to a fire hazard	fire detection data
measured physical parameter related to a gas hazard	inflammable/explosive gas detection data
real time clock data	real-time data
residual energy of a power source	battery status data
site specific configuration	function configuration data
site/device identifier	device identifier data
system configuration	function configuration data
the time of a logged event	real-time data and logging data

Table H.4: Mapping of FGS specific function assets to function assets

FGS specific function assets	Function assets
actuator control function (ventilation or other ancillary device)	actuator control function or other products' configuration function
configuration function	data modification function
fault detection function	external sensing function
fire/gas alarm notification function	data communication function and/or fire/gas alarm function
hazard detection function	external sensing function
interconnection function	connection function
logging function	data modification function and potentially data communication function
power supply function	power supply function
real time clock	external sensing function
software update mechanism	data modification function and data communication function
sounder	fire/gas alarm function
user access control function	security function
user interface function	data presenting function

H.4 Terminology mappings for intrusion and hold-up alarm systems (I&HAS)

The terminology mappings for I&HASs based EN 50131 series (EN 50131-1 [i.23], EN 50131-2-2 [i.24], EN 50131-2-3 [i.25], EN 50131-2-4 [i.26], EN 50131-2-5 [i.27], EN 50131-2-6 [i.28], EN 50131-2-7-1 [i.29], EN 50131-2-7-2 [i.30], EN 50131-2-7-3 [i.31], EN 50131-2-8 [i.32], EN 50131-2-10 [i.33], EN 50131-3 [i.34], EN 50131-4 [i.35], EN 50131-5-3 [i.36], EN 50131-6 [i.37], EN 50131-8 [i.38], EN 50131-10 [i.39] and EN 50131-13 [i.40]) of standards are provided in tables H.5 and H.6.

Table H.5: Mapping of I&HAS specific data assets to data assets

I&HAS specific data assets	Data assets
alarm state of a zone	state data or intrusion detection data or hold-up detection data
authentication credentials	cryptographic security parameter or identity data for authentication
authorised users identifiers	identity data for authentication
command of a door lock	actuator control data
communicated multimedia data streams	private audio data and/or private video data
door/window status	window/door opening status data
fault detection data	function fault detection data
fault state of a zone	state data or function fault detection data
hold-up detection data	hold-up detection data
intrusion detection data	intrusion detection data
logged event	logging data
measured physical parameter related to an intrusion	intrusion detection data
real time clock data	real-time data
residual energy of a power source	battery status data
site specific configuration	function configuration data
site/device identifier	device identifier data
system configuration	function configuration data
tamper detection data	object tamper detection data
tamper state of a zone	state data or object tamper detection data
the time of a logged event	real-time data and logging data

Table H.6: Mapping of I&HAS specific function assets to function assets

I&HAS specific function assets	Function assets
audible notification	intrusion and hold up alarm function
configuration function	data modification function
fault detection function	external sensing function
hold-up detection function	external sensing function
indicating function	data presenting function
interconnection function	connection function
intrusion detection function	external sensing function
intrusion/hold-up notification function	data communication function and/or intrusion and hold up alarm function
localisation function	external sensing function
logging function	data modification function and potentially data communication function
multimedia input function	external sensing function or data communication function
multimedia output function	data presenting function or data communication function
power supply function	power supply function
real time clock	external sensing function
tamper security function	security function
user access control function	security function

H.5 Terminology mappings for social alarm systems (SAS)

Social alarm systems and related products are typically delivered in different configurations, and each configuration has distinct system boundaries and risk considerations. Defining specific profiles supports the consist and unambiguous application of the present document to a given product that is part of a social alarm systems solution. The social alarm system Profiles are defined as follows:

- SAS P1 - Local Unit + Trigger (Basic Kit):
  - Description: A standalone social alarm device (Local Unit or controller) provided with at least one personal trigger (e.g. pendant or wrist trigger). The local unit (which may be a base console or integrated wearable device) communicates directly with an alarm receiving centre (ARC) or designated responder via a telecommunication network (analog phone line, cellular, IP) without relying on any manufacturer-managed cloud service.
  - Risk considerations: The P1 profile covers the fundamental life-safety critical path of alarm triggering, signal transmission, and two-way voice communication. The immediate availability and integrity of alarm functions are paramount, as this device is the user's primary link to emergency assistance. Security measures (such as authentication credentials or encryption keys) reside on the device and are protected, but there is no persistent cloud connectivity requiring maintenance of a platform.
- SAS P2 - Local Unit + Trigger + Management Platform:
  - Description: A connected social alarm solution that includes the P1 device kit and an associated management platform (DMP/DPMP or Alarm Management Service) provided by the manufacturer for remote configuration, monitoring, or value-added functionalities. The local alarm unit still communicates alarms directly to the ARC (as in P1), but it also interacts with the cloud platform for non-time-critical services (e.g. device provisioning, status monitoring, software updates, or possibly enhanced alarm routing logic).

  - Risk considerations: The P2 profile introduces a remote platform into the social alarm ecosystem. While the core alarm delivery to the ARC remains time-critical and is not hindered (per EN 50134-5 [i.44], security measures or platform outages typically do not prevent alarm transmission), the platform brings additional security assets (e.g. cloud credentials, APIs, and cryptographic links) and functions (remote access to configure/update devices). Integrity of the platform's interactions is critical - a malicious configuration change or compromised platform credential could disrupt alarms or privacy. However, because alarms can typically still reach the ARC even if the platform is temporarily unavailable, the immediate availability of the platform is generally less critical (often low for time-critical availability) than the local alarm path. Extended loss or compromise of the platform (e.g. a prolonged outage or malicious takeover) can degrade service (no remote supervision or updates, possible loss of advanced features), so these aspects carry moderate impact on availability and integrity in P2.

- SAS P3 - Additional Trigger Device (Peripheral Only):

  - Description: A standalone alarm trigger unit (wireless pendant, wearable fall detector, smoke/CO sensor, etc.) sold separately to be paired with an social alarm local unit. This profile covers individual sensors/trigger devices that cannot communicate with an ARC on their own but form part of a larger alarm system when enrolled to an social alarm controller (P1, P2 or S1).

  - Risk considerations: The P3 profile has a narrower scope (no controller or network interface of its own), but its functions are still safety-critical within the system: a trigger device generates an alarm signal reliably when needed and maintain its link (radio or wired) to the controller. The integrity of trigger signals and availability of the trigger function are typically High impact - a false signal can cause needless emergency responses or desensitisation to alarms, while a missed or failed trigger can mean a real emergency goes unanswered. Confidentiality concerns are generally lower in P3 because these devices hold minimal personal data (they usually transmit simple coded alerts and status, without storing user-specific information). Many P3 devices are battery-powered and wireless, so supervision (heartbeat) signals and battery status alerts are crucial: loss of these functions would leave the user unprotected without warning. Overall, P3 emphasizes the reliability of alarm initiation and the secure pairing with the controller, while aspects related to long-term data storage or user databases do not apply.

- SAS S1 - TaaS (End-to-End telecare as a service):

  - Description: A complete social alarm service provided by a single supplier, typically to an alarm monitoring provider or directly to end-users, encompassing the local alarm device (with triggers), the communication network (e.g. managed cellular or IP connectivity), optional platform services, and the 24/7 alarm monitoring centre (ARC and response operator service). This profile effectively bundles multiple components into one offer - it is an social alarm system profile rather than just a product.

  - Risk considerations: The S1 profile inherits all the critical aspects of P1 and P2, and extends them to the service layer. Because the supplier operates the ARC and possibly dedicated network infrastructure, all personal data and alarm handling functions are in scope. This means additional high-confidentiality assets (e.g. sensitive client records, medical information, voice recordings of emergency calls), and a need for comprehensive audit and operator access control. The availability requirements are highest in S1, since any failure in any part of the chain (device, platform, or ARC) can directly compromise the emergency response. Every aspect of the alarm service is both resilient and secure: from the user's trigger, through secure communications, to correct alarm handling and dispatch of help. In S1, confidentiality demands also peak because the service provider holds detailed personal information and potentially health-related data, which are protected. S1 thus represents the full end-to-end risk scenario for social alarms under the CRA, combining device-level and service-level considerations.

The terminology mappings for SASs based EN 50134 series (EN 50134-1 [i.41], EN 50134-2 [i.42], EN 50134-3 [i.43], EN 50134-5 [i.44] and EN 50134-7 [i.45]) of standards are provided in tables H.7 and H.8.

Table H.7: Mapping of SAS specific data assets to data assets

SAS specific data assets	Data assets
acknowledgement / receipt confirmation indication (bidirectional trigger where supported; alarm acknowledgement timestamps) [SA P1, SA P2, SA P3, SA S1]	actuator control data and/or function configuration data and/or other products' function configuration data
alarm trigger event (e.g. pendant press; automatic trigger event such as fall) [SA P1, SA P2, SA P3, SA S1]	state data and/or human emergency detection data
authorised contact lists/responder identifiers [SA P2, SA S1]	personal contact data and/or identity data for authentication and/or device identifier data
client/service user records (ARC-side data store, TaaS end-to-end service) [SA S1]	human emergency detection data and/or function fault detection data and/or object tamper detection data and/or battery status data and/or others
configuration data [SA P2, SA S1]	function configuration data and/or other products' function configuration data
control commands (e.g. remote reset/cancel of alarm unit; acknowledge/cancel commands from authorised entities) [SA P1, SA P2, SA S1]	actuator control data and/or function configuration data and/or other products' function configuration data
cryptographic security parameters (keys, certificates, tokens) used for secure communications/storage (e.g. TLS/VPN key material) [SA P1, SA P2, SA S1]	cryptographic security parameter
device ID [SA P1, SA P2, SA P3, SA S1]	device identifier data
distributed logs for supervision and audit [SA P1, SA P2, SA P3, SA S1]	logging data
fault detection data (e.g. power failure, communication failure, sensor out-of-range, tamper where implemented) [SA P1, SA P2, SA P3, SA S1]	function fault detection data
human fall detection data [SA P1, SA P2, SA S1]	human emergency detection data
location information for mobile/wearable SA (conditional: only where location is used; include unknown/unavailable/stale state) [SA P1, SA P2, SA S1]	entity's location data
low battery warning signals from LUC or trigger devices [SA P1, SA P2, SA P3, SA S1]	battery status data
presence / heartbeat [SA P1, SA P2, SA P3, SA S1]	health data and/or human emergency detection data
real time clock data [SA P1, SA P2, SA P3, SA S1]	real-time data
security credentials for system access and authentication (installer/operator credentials; device/ARC authentication parameters) [SA P1, SA P2, SA S1]	cryptographic security parameter
service user identifiers where stored (often pseudonymised) [SA P2, SA S1]	personal contact data and/or identity data for authentication and/or device identifier data
status indicators (alarm active/inactive; fault/tamper; battery low) [SA P1, SA P2, SA P3, SA S1]	state data and/or human emergency detection data and/or function fault detection data and/or object tamper detection data and/or battery status data and/or others
system logs [SA P1, SA P2, SA P3, SA S1]	logging data
timestamps for alarms and acknowledgements [SA P1, SA P2, SA P3, SA S1]	real-time data
trigger device identification / coded identifier used to prevent unwanted triggering in adjacent systems (wire-free triggers)	actuator control data and/or function configuration data and/or other products' function configuration data
trigger device periodic presence / heartbeat signal (wire-free triggers) [SA P1, SA P3, SA S1]	health data and/or human emergency detection data
two-way voice communication media during an alarm call (service user ↔ monitoring centre) [SA P1, SA P2, SA S1]	private audio data
video image transmission during an alarm call (conditional: only where video is supported) [SA P1, SA P2, SA S1]	private video data

Table H.8: Mapping of SAS specific function assets to function assets

SAS specific function assets	Function assets
automatic triggering / sensor event detection (e.g. fall detection; smoke/CO; bed/chair; door sensors) (conditional: only where implemented) [SA P1, SA P2, SA P3, SA S1]	external sensing function
configuration function (device/service configuration via local programming and/or DMP/DPMP where present) [SA P2, SA S1]	data modification function
connection function (establish/test communication capability via machine interface; commissioning tests) [SA P1, SA P2, SA P3, SA S1]	connection function
cryptographic function (TLS/VPN/secure storage mechanisms where implemented) [SA P1, SA P2, SA S1]	security function
fault detection function (supervision/health monitoring of communications, power, trigger link status, platform status where applicable) [SA P1, SA P2, SA P3, SA S1]	external sensing function
interconnection function (radio/hardwired trigger links; WAN connectivity to ARC; platform interconnections) [SA P1, SA P2, SA P3, SA S1]	connection function and/or data communication function
localisation function (mobile/wearable SA location) (conditional: only where location is used) [SA P1, SA P2, SA S1]	external sensing function
logging function (event recording, audit trail, retention) [SA P1, SA P2, SA P3, SA S1]	data modification function and potentially data communication function
power supply function [SA P1, SA P2, SA P3, SA S1]	power supply function
triggering function / control function (alarm initiation, escalation, cancel/ack flows; includes peripheral trigger role) [SA P1, SA P2, SA P3, SA S1]	external sensing function and/or social alarm function and/or actuator control function and/or others
two-way communication media processing (video) (conditional: only where video supported) [SA P1, SA P2, SA S1]	external sensing function and data communication function and data presenting function
two-way communication media processing (voice) [SA P1, SA P2, SA S1]	external sensing function and data communication function and data presenting function
user access control function (operator/admin access control where implemented) [SA P1, SA P2, SA S1]	security function
visual and audible indicators / operator presentation (local indications; ARC/operator data presentation) [SA P1, SA P2, SA S1]	data presenting function and/or social alarm function and/or physical security notification function

Annexes I to J: Void

Annex K (normative): Generic cryptographic requirements and assessment

K.1 Cryptography

K.1.1 [CRY-SOTA] Requirement

The SHPSF'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 Agreed Cryptographic Mechanisms [1]; or

2) ACM-extended: the cryptographic mechanism is not listed Agreed Cryptographic Mechanisms [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 SHPSF 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 Agreed Cryptographic Mechanisms [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 SHPSF functions

3) Interoperability-based: the cryptographic mechanism is listed in clause K.4.2 as an interoperability-based cryptographic mechanism for specific SHPSF function(s) and external specification(s) or external requirement(s).

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.

NOTE 1: The reference to the SHPSF's default configuration is intended to define a clear and assessable baseline, corresponding to the configuration in which the SHPSF is placed on the market. The SHPSF can provide several configurations that fulfil the requirement.

NOTE 2: For SHPSFs supplied as hardware platforms or components to be configured by an integrator, references in this annex to the SHPSF's default configuration refer to the configuration specified for the intended operational use of the SHPSF after integration, including the relevant integration assumptions and configuration constraints.

NOTE 3: The applicable Agreed Cryptographic Mechanisms [1] catalogue version is identified in the normative references of the present document. The lifecycle treatment of mechanisms affected by Agreed Cryptographic Mechanisms [1] 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 SHPSF, and which requires the use of a specific cryptographic mechanism for the SHPSF 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.

K.1.2 Assessment criteria

K.1.2.1 Assessment criteria for [CRY-SOTA] concerning ACM-listed cryptographic mechanisms

Assessment reference:

[CRY-SOTA] concerning ACM-listed cryptographic mechanisms

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 Agreed Cryptographic Mechanisms [1].

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 Agreed Cryptographic Mechanisms [1] entry.

Assessment activities:

The assessment shall include verification that:

- each cryptographic mechanism claimed under clause K.1.1 item 1) is identified by reference to a relevant Agreed Cryptographic Mechanisms [1] entry; and
- the Agreed Cryptographic Mechanisms [1] entry corresponds to the cryptographic mechanism used in the product's default configuration, including relevant parameters where applicable; and
- where the Agreed Cryptographic Mechanisms [1] entry includes lifecycle information, such as expiry date, deprecation date, migration condition or usage limitation, this information is reflected in the documentation.

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.

Assessment evidence:

The assessment evidence shall include, as applicable:

- description of the product's default configuration; and
- list of cryptographic mechanisms claimed under clause K.1.1 item 1); and

- references to the relevant Agreed Cryptographic Mechanisms [1] entries; and
- relevant parameters, profiles, cipher suites or configuration constraints, where applicable; and
- relevant lifecycle information from the Agreed Cryptographic Mechanisms [1] catalogue, where applicable.

K.1.2.2 Assessment criteria for [CRY-SOTA] concerning ACM-extended cryptographic mechanisms

Assessment reference:

[CRY-SOTA] concerning ACM-extended cryptographic mechanisms

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).

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:
  - the relevant entry in clause K.3.2; or
  - evidence that the cryptographic mechanism fulfils all applicable criteria in clause K.1.1 item 2.b.

Assessment activities:

The assessment shall include verification that:

- 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; and
- 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; and
- 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; and
- 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; and
- 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; and
- where technically feasible, the cryptographic mechanism, parameters and configuration identified in the documentation correspond to the assessed product configuration.

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.

Assessment evidence:

The assessment evidence shall include, as applicable:

- description of the product's default configuration; and
- list of cryptographic mechanisms claimed under clause K.1.1 item 2); and
- reference to the relevant entry in clause K.3.2, where the mechanism is listed in clause K.3.2; and
- 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; and
- identification of the related product function using the cryptographic mechanism and the use case where applicable; and
- relevant characteristics, parameters, profiles, cipher suites or configuration constraints, where applicable; and
- 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.1.2.3 Assessment criteria for [CRY-SOTA] concerning interoperability-based cryptographic mechanisms

Assessment reference:

[CRY-SOTA] concerning interoperability-based cryptographic mechanisms

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.

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.

Assessment activities:

The assessment shall include verification that:

- each cryptographic mechanism claimed under clause K.1.1 item 3) is listed in clause K.4.2 as an interoperability-based cryptographic mechanism; and
- the cryptographic mechanism used by the product corresponds to the cryptographic mechanism listed in clause K.4.2; and
- 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; and
- 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; and
- 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; and
- 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; and

- where technically feasible, the cryptographic mechanism, parameters and configuration identified in the documentation correspond to the assessed product configuration.

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.

Assessment evidence:

The assessment evidence shall include, as applicable:

- description of the product's default configuration; and
- list of cryptographic mechanisms claimed under clause K.1.1 item 3); and
- reference to the relevant entry in clause K.4.2; and
- identification of the related product function using the cryptographic mechanism and the use case where applicable; and
- identification of the external specification or external requirement requiring use of the cryptographic mechanism; and
- relevant characteristics, parameters, profiles, cipher suites or configuration constraints, where applicable; and
- evidence that the cryptographic mechanism is used in accordance with the conditions or limitations specified in clause K.4.2.

K.2 Crypto agility

K.2.1 [CRY-AGIL] Requirement

Where the SHPSF's default configuration uses a cryptographic mechanism for which the Agreed Cryptographic Mechanisms [1] catalogue, or the present document, specifies a deprecation date, expiry date, migration condition or usage limitation falling within the intended lifetime of the SHPSF, the SHPSF shall provide means for addressing the affected cryptographic mechanism by one or more of the following:

- 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.

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 Agreed Cryptographic Mechanisms [1] catalogue or by the present document. However, hybridization 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. Hybridization is not assumed to mitigate the deprecation of a constituent primitive unless the Agreed Cryptographic Mechanisms [1] 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 Agreed Cryptographic Mechanisms [1] 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 criteria for [CRY-AGIL]

Assessment reference:

[CRY-AGIL]

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 Agreed Cryptographic Mechanisms [1] 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.

Assessment preparation:

- Preconditions for the assessment: The product's default configuration shall be used for the assessment.
- The documentation shall identify:
  - the intended lifetime of the product;
  - the cryptographic mechanisms used in the product's default configuration;
  - the related product function(s) for each cryptographic mechanism;
  - the lifecycle information applicable to each cryptographic mechanism, where specified by the Agreed Cryptographic Mechanisms [1] catalogue or the present document, including any deprecation date, expiry date, migration condition or usage limitation.

Assessment activities:

The assessment shall include verification that:

- for each cryptographic mechanism used in the product's default configuration, the lifecycle information specified by the Agreed Cryptographic Mechanisms [1] catalogue or the present document has been identified, where such information is specified; and
- where the Agreed Cryptographic Mechanisms [1] 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; and
- 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; and
- 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.

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.

Assessment evidence:

The assessment evidence shall include, as applicable:

- documentation of the intended lifetime of the product; and
- list of cryptographic mechanisms used in the product's default configuration; and
- identification of the related product function(s) for each cryptographic mechanism; and
- references to the Agreed Cryptographic Mechanisms [1] catalogue entry or to the provision of the present document used to determine lifecycle information, where applicable; and
- identification of any deprecation date, expiry date, migration condition or usage limitation falling within the intended lifetime of the product; and
- 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.3 ACM-extended cryptographic mechanisms

K.3.1 [CRY-ACM-EXT] Requirement

Where the SHPSF'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: 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 [CRY-INTOP] Requirement

Where the SHPSF'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: 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 SHPSF 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

History

Version	Date	Status
V1.0.0	July 2026	SRdAP process EV 20261012: 2026-07-20 to 2026-10-12