ETSI TS 104 013 V1.1.1 (2026-01)

TECHNICAL SPECIFICATION

Cyber Security (CYBER);
EUCC PP for ONDS management protocols and services

Reference
DTS/CYBER-00121

Keywords
cybersecurity, network management, optical

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 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.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

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 Optical Network Device Security (ONDS) suite of documents is developed as an interlinked collection, shown in figure 1.

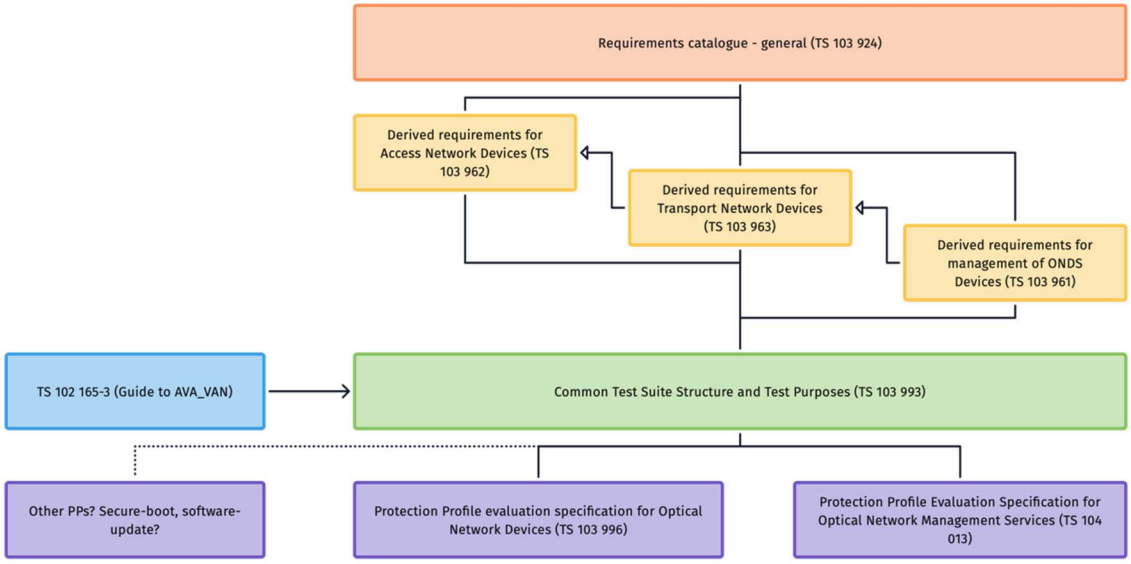

Figure 1: Document structure for Optical Network Device Security

Each of ETSI TS 103 962 [2], ETSI TS 103 963 [3] and ETSI TS 103 961 [1] expand upon the requirements identified in the common catalogue of ETSI TS 103 924 [12]. In the definition of detailed provisions, ETSI TS 103 962 [2] acts as the master document with each of the present document and ETSI TS 103 961 [1] identifying further specializations.

To drive the evaluation and test of the ONDS suite a common Test Suite Structure and Test Purposes definition is given in ETSI TS 103 993 [i.10], and from that is derived a specification of the evaluation assessments to be applied is given in the form of a partial protection profile mapped to ETSI TS 103 962 [2] and ETSI TS 103 963 [3] in ETSI TS 103 996 [11], and to ETSI TS 103 961 [1] in ETSI TS 104 013 (the present document).

NOTE: All of the documents identified in Figure 1 act together to fully define the requirements, test and evaluation for placing an ONDS device on the market.

1 Scope

The present document is a protection profile for ONDS management of devices as described in ETSI TS 103 961 [1] and supporting management of devices described in ETSI TS 103 962 [2], ETSI TS 103 963 [3]. The Security Functional Requirements (SFRs) are extended from the Common Criteria Part 2 [5] and defined in support of the AVA_VAN class from Common Criteria Part 3 [6].

NOTE 1: The present document adopts the style and much of the structure of a PP adapted to conform to the ETSI Stylesheet.

NOTE 2: The present document is structured in such a way to form part of the EUCC [i.15] submission.

NOTE 3: The present document addresses the assurance levels identified in CSA [i.13] for EUCC [i.15] as Substantial (Article 52.6 of [i.13]).

NOTE 4: In the present document the requirements from [1] and [2] in the conventional ETSI format are highlighted against the most relevant SFRs from [5], in clauses 9 and 10 and in Annex B.

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] ETSI TS 103 961: "CYBER; Optical Network and Device Security; Security provisions for the management of Optical Network devices and services".

[2] ETSI TS 103 962: "CYBER; Optical Network and Device Security; Security provisions in Optical Access Network Devices".

[3] ETSI TS 103 963: "CYBER; Optical Network and Device Security; Security provisions in transport network devices".

[4] ISO/IEC 15408-1:2022: " Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general mode".

NOTE: This reference is also available as "Common Criteria for Information Technology, Security Evaluation, Part 1: Introduction and general model, November 2022, Revision 1, CCMB-2022-11-001".

[5] ISO/IEC 15408-2:2022: "Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components".

NOTE: This reference is also available as "Common Criteria for Information Technology, Security Evaluation, Part 2: Security functional components, November 2022, Revision 1, CCMB-2022-11-002".

[6] ISO/IEC 15408-3:2022: Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components".

NOTE: This reference is also available as "Common Criteria for Information Technology, Security Evaluation, Part 3: Security assurance components, November 2022, Revision 1, CCMB-2022-11-003".

[7] ISO/IEC 15408-4:2022: "Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities".

NOTE: This reference is also available as "Common Criteria for Information Technology, Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, November 2022, Revision 1, CCMB-2022-11-004".

[8] ISO/IEC 15408-5:2022: "Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements".

NOTE: This reference is also available as "Common Criteria for Information Technology, Security Evaluation, Part 5: Pre-defined packages of security requirements, November 2022, Revision 1, CCMB-2022-11-005".

[9] ISO/IEC 18045:2022: " Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation.

NOTE: This reference is also available as "Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, November 2022, Revision 1, CCMB-2022-11-006".

[10] ETSI TS 102 165-3: "Cyber Security (CYBER); Methods and Protocols for Security, Part 3: Vulnerability Assessment extension for TVRA".

[11] ETSI TS 103 996: "Cyber Security (CYBER); EUCC PP for Optical Network and Device Security (ONDS)".

[12] ETSI TS 103 924: "Optical Network and Device Security; Catalogue of Requirements".

[13] NIST SP 800-90A Rev. 1: "Recommendation for Random Number Generation Using Deterministic Random Bit Generators".

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] ETSI TS 102 165-1: "Cyber Security (CYBER); Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[i.2] ETSI TR 103 838: "Cyber Security; Guide to Coordinated Vulnerability Disclosure".

[i.3] IETF RFC 3164: "The BSD syslog Protocol".

[i.4] IETF RFC 5434: "The Syslog Protocol".

[i.5] BSI TR-02102-1 "Cryptographic Mechanisms: Recommendations and Key Lengths", version 2025-1.

[i.6] ETSI TS 103 994-1: "Cyber Security (CYBER); Privileged Access Workstations; Part 1: Physical Device".

[i.7] ETSI TS 103 305-1: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.8] ETSI TS 103 645: "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

NOTE: The above TS is periodically published as ETSI EN 303 645.

[i.9] Directive (EU) 2022/2555 of the European Parliament and Council on measures for a high common level of cybersecurity across the Union, (NIS2 Directive).

[i.10] ETSI TS 103 993: "Cyber Security (CYBER); ONDS Test Suite Structure and Test Purposes".

[i.11] ETSI TS 103 486: "CYBER; Identity Management and Discovery for IoT".

[i.12] ETSI TS 103 701: "Cyber Security (CYBER); Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements".

[i.13] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17. April 2019 on ENISA and on information and communication technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[i.14] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

[i.15] Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 103 961 [1], ETSI TS 103 962 [2], ETSI TS 103 963 [3] and the following apply:

substantial assurance level: assurance that the ICT products, ICT services and ICT processes where the corresponding security requirements, including security functionalities, are provided at a level intended to minimize the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources

NOTE 1: A contextual definition is given in CSA Article 52.6 [i.13].

NOTE 2: A mapping from the CSA [i.13] definition to the metrics for risk analysis is given in ETSI TS 102 165-3 [10] and in ETSI TS 102 165-1 [i.1].

3.2 Symbols

Void.

3.3 Abbreviations

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

AAT	Attribute Authority Tree
AES	Advanced Encryption System
CC	Common Criteria
CRA	Cyber Resilience Act
CSA	Cyber Security Act
DoS	Denial of Service

EAL	Evaluation Assurance Level
EUCC	Common Criteria-based European cybersecurity certification scheme
FCAPS	Fault Configuration Accounting Performance Security
GPDR	General Data Protection Regulation
HW	Hardware
ICT	Information Communications Technology
IoT	Internet of Things
IP	Internet Protocol
IXIT	Implementation eXtra Information for Testing
NE	Network Element
NMS	Network Management System
NTP	Network Time Protocol
O&M	Operation and Maintenance
OAN	Optical Access Network
OID	Object Identifier
ON	Optical Network
OND	Optical Network Device
ONDS	Optical Network and Device Security
OSS	Operations Support System
PKC	Public Key Certificate
PKI	Public Key Infrastructure
PP	Protection Profile
RtS	Root of Trust for Storage
SAR	Security Assurance Requirement
SBOM	Software Bill of Materials
SFP	Security Function Policy
SFR	Security Functional Requirement
SPD	Security Problem Definition
ST	Security Target
SUT	System Under Test
SW	Software
TLS	Transport Layer Security
TOE	Target of Evaluation
ToE	Target of Evaluation
TSF	TOE Security Function
VIAR	Vulnerability Impact Analysis Report

3.4 Notations convention for SFRs and SARs

For the purposes of the present document, the following notations, symbols and structural conventions from [5] apply:

- ~~Strikethrough~~ indicates text replaced with alternative text as a refinement.
- [Underlined text in brackets] indicates additional text provided as a refinement.

NOTE 1: It is recognized that the convention above from [5] clashes with the ETSI convention for references.

- If not being the headline of the SFR itself, **bold** text indicates the completion of an assignment.
- ***Italicized and bold*** text indicates the completion of a selection.
- Iteration/Identifier indicates an element of the iteration, whereas the identifier distinguishes the different iterations.
- Normal text applies unchanged from the SFR definition in [5].
- Begin and end of application- and general notes are marked in *italic letters* and are given below the according SFR or SAR definition. General notes are informative only.

NOTE 2: It is recognized that this is inconsistent with the use of notes in ETSI's stylesheet.

- Begin and end of evaluator action elements are marked in *italic and underlined letters* and are given below the SFR definition. An evaluator action element should be understood as guidance for the evaluation action of a certain requirement detail.

4 Overview of protection profile and assurance

4.1 General concepts

The present document defines an EUCC conformant Protection Profile (PP) for the purpose of evaluation of the security provisions given for the management of ONDS devices established in ETSI TS 103 961 [1]. The PP extension addresses test cases for each requirement with the purpose of advising the evaluator and developer of how a pass verdict for conformance is to be achieved.

The PP described in the present document is documented to be consistent with at least Substantial level as defined in the EU Cyber Security Act (CSA) [i.13] and has been designed to be consistent with the requirements of the Common Criteria-based European cybersecurity certification scheme (EUCC) [i.15].

A PP is defined as an implementation-independent statement of security requirements for a Target Of Evaluation (TOE) addressing a particular type of device by ISO/IEC 15408 [4], [5], [6], [7], [8] (and in the corresponding text from the Common Criteria group). A PP may inherit requirements from one or more other PPs.

NOTE 1: In like manner to a PP an ETSI Technical Specification defines an implementation-independent statement of requirements, where these requirements are stated for the present document in ETSI TS 103 961 [1].

NOTE 2: The term TOE has a similar meaning to System Under Test (SUT) that is conventionally used in ETSI test documents.

NOTE 3: In ETSI TS 102 165-1 [i.1] the use of ToE is being deprecated in favour of a more general and wider system role of identification of the attack surface of a system or component although there remains a close mapping to the ToE in use in [4].

In the convention of PP it is necessary to identify Security Functional Requirements (SFRs), which contribute to fulfil the security requirements for protection of the TOE identified in either the Security Problem Definition (SPD) in clause 6, or in the Protection Profile (PP) in clauses 7 through 11. In each case the base requirements for the management of ONDS devices established in ETSI TS 103 961 [1] apply, and are mapped to the relevant SFRs in Annex A and to the Test Purposes defined in ETSI TS 103 993 [i.10] in Annex C.

The structure of a PP is defined in Annex B of [4] and shall normally contain the elements outlined in Figure 2.

NOTE 4: In ETSI's convention it is normal that the security objectives and security requirements are made by reference to other documents, e.g. ETSI TS 103 961 [1] which is not recommended in CC, although for the present document the ETSI convention is maintained as much as is practical.

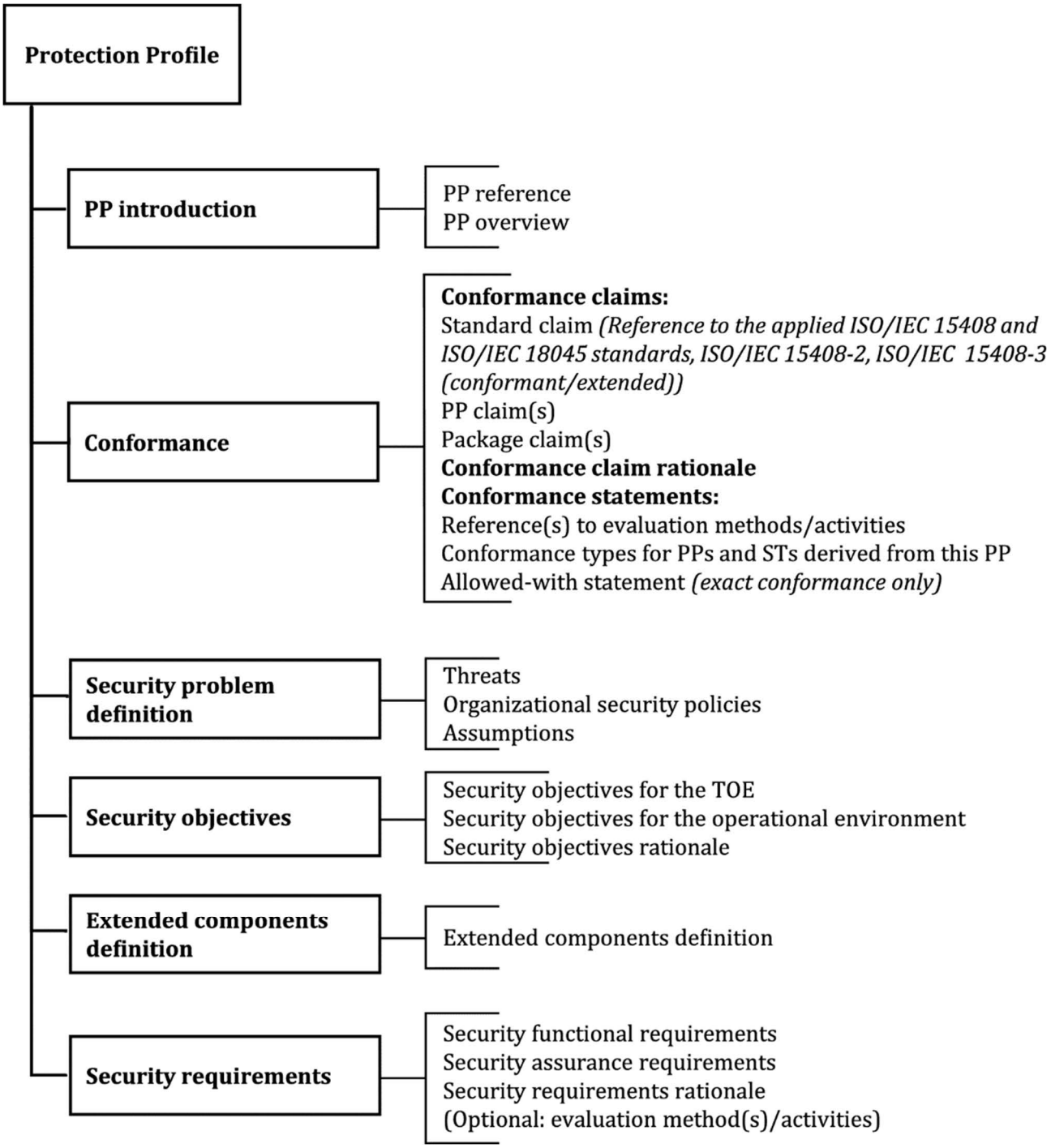

Figure 2: Contents of a Protection Profile from CC Part 1, annex B [4]

The structure of the PP shown in Figure 2 places the security problem above the security objectives. An alternative convention is often followed in the ETSI standards process wherein the system objective is met by the system design. The threats are against the system objectives (see ETSI TS 102 165-1 [i.1] and Figure 3) and those threats, and their mitigation, is the security problem to be solved by the identification and implementation of mechanisms in support of the security requirements. The present document follows the broad model of ETSI TS 102 165-1 [i.1] mapped to the PP content structure of Figure 2.

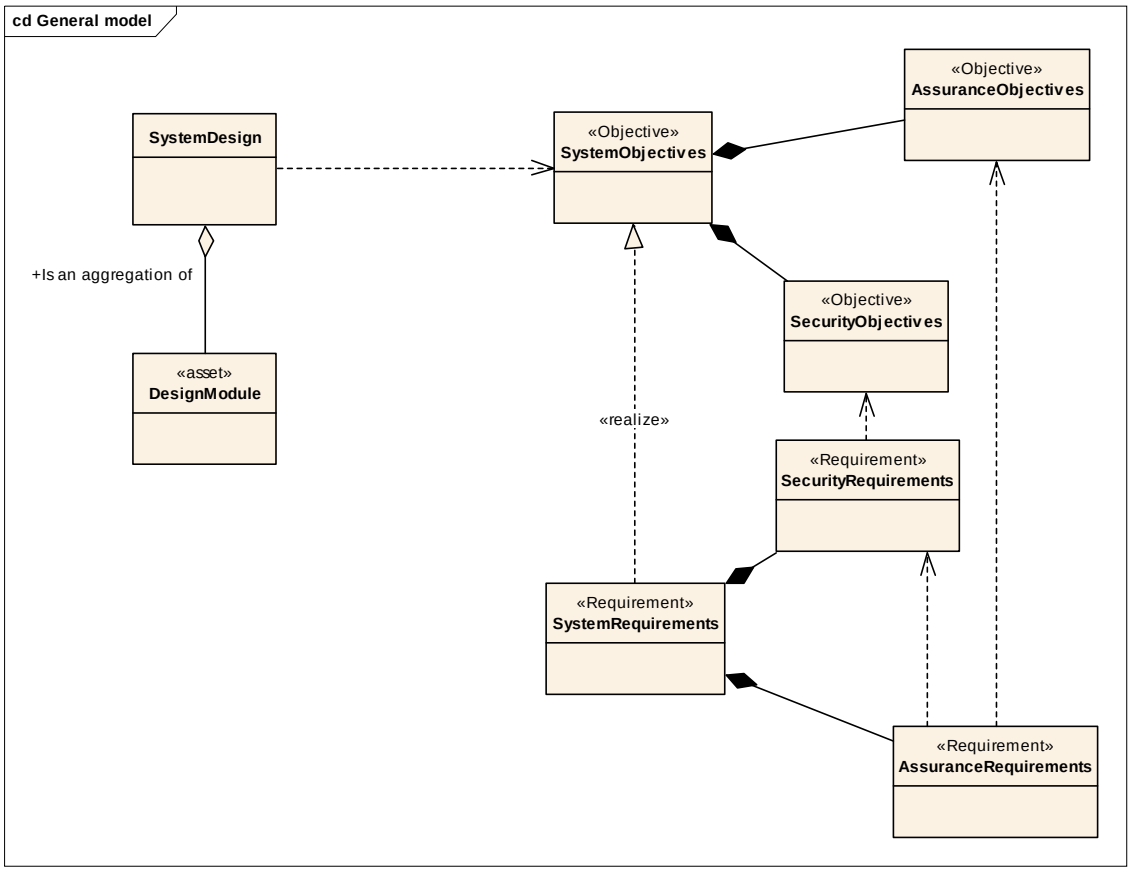

Figure 3: Relationship between system design, objectives and requirements from [i.1]

For the purposes of the present document, and from the expectations of the market position in core networks that may be classified as critical infrastructure, the assurance level identified in CSA [i.13] for EUCC [i.15] as Substantial (Article 52.6 of [i.13]) apply.

Quote: *"A European cybersecurity certificate that refers to assurance level '**substantial**' shall provide assurance that the ICT products, ICT services and ICT processes for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimize the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities. Where any such evaluation activities are not appropriate, substitute evaluation activities with equivalent effect shall be undertaken (from [i.13])."*

4.2 Alignment to expectation of APE class of CC-Part 3

4.2.1 Overview

The present document, including the referenced content of [1], is written to conform to the requirements that allow its evaluation as a Protection Profile as outlined in CC-Part 3 [6] for class APE as modified for EUCC [i.15].

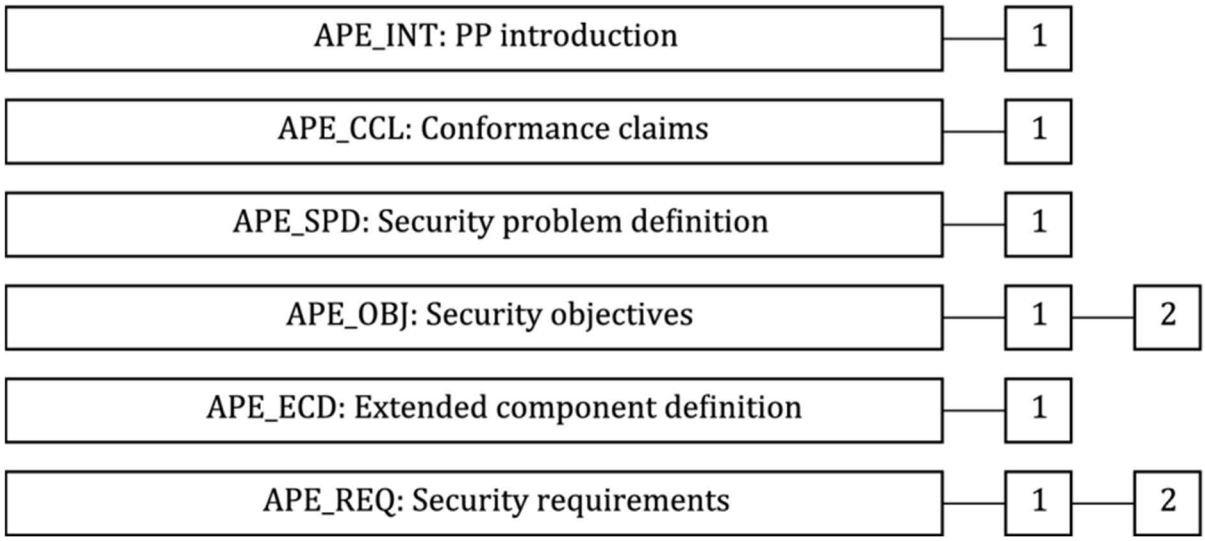

Figure 4: Components of APE class from CC-Part-3 [6]

4.2.2 Conformance Claim against APE_INT

The present document is made with respect to the provisions of [1].

The unique EUCC/PP reference is to the full title and version number of the present document:

- ETSI TS 103 961 [1].

NOTE: The certified version of the present document is registered with ENISA under the EUCC scheme.

4.2.3 Claim against APE_CCL

The present PP was built with, and claims conformance to, the Common Criteria for Information Technology Security Evaluation (in version 2022, in revision 1, as of November 2022, for all parts: [4], [5], [6], [7] and [8]). In addition, the present document claims conformance to the base requirements established in the ONDS requirements catalogue in ETSI TS 103 924 [12] and their specialization in ETSI TS 103 961 [1].

The Protection Profile (PP) defined in the present document claims to be conformant with the Common Criteria version 2022 Revision 1 as of November 2022 with the SAR extension as follows:

- Part 3: ISO/IEC 15408-3 [6] extended, ALC_SWU Software Update Management (see clause 10.3.1.1).

The chosen Evaluation Assurance Level (EAL) is augmented with ALC_FLR.2, which is defined in ISO/IEC 15408-3 [6].

The underlying methodology to be considered for the present PP is the Common Methodology for Information Technology Security Evaluation in version 2022, in revision 1, as of November 2022, [6] as applicable to the EUCC [i.15] programme.

NOTE: As stated above (scope statement (clause 1) and in clause 4.1) the specific assurance level claim of the present document is to level substantial as defined in Article 52 of [i.13].

4.2.4 Claim against APE_SPD

The security problem is defined in the reference documents ETSI TS 103 961 [1], and summarized in clause 6 of the present document.

4.2.5 Claim against APE_OBJ

The security objectives are defined in the reference documents ETSI TS 103 961 [1], and summarized in clauses 6.5 and 6.6 of the present document.

4.2.6 Claim against APE_ECD

The package claim, taken from ISO/IEC 15408-5 [8] of the present PP is:

EAL3 augmented with ALC_FLR.2

AVA_VAN.2 [8], Vulnerability analysis methodically tested and checked, is included (see also clause 4.4 below).

NOTE: The expectation of Substantial defined in Article 53 of [i.13] is that AVA_VAN.2 as a minimum is required.

This PP is conforming to assurance package EAL3 augmented with ALC_FLR.2. However, the ST author may choose to claim additional or hierarchically stronger SFRs and SARs. This does not violate the conformance claim of the PP.

4.2.7 Claim against APE_REQ

The security requirements are defined in the reference documents [1], and stated in SFR format in clauses 8 and 9 of the present document (Annex A provides a mapping between the format used in the reference documents and that of PP-Part 2). Assurance claims are defined in clause 10 of the present document.

4.3 PP Claim

The present PP requires strict conformance of the ST or PP claiming conformance to the present document.

The present PP in all parts do not claim conformance to any other PP.

4.4 Claim against the AVA_VAN class

The EUCC scheme adopts provisions of the AVA_VAN class from CC Part 3 [6] specifically mapped to the metrics defined in ETSI TS 102 165-1 [i.1] for attack potential as shown in Table 1 and these are mapped to the CSA expectation for each of Basic, Substantial and High.

Table 1: Vulnerability rating

Attack potential values	Attack potential required to exploit attack	Resistant to attacker with attack potential of	AVA_VAN	CSA [i.13] rating
0 to 9	Basic	No rating		CSA-Basic
10 to 13	Enhanced-basic	Basic	AVA_VAN.1 and AVA_VAN.2	CSA-Substantial
14 to 19	Moderate	Enhanced basic	AVA_VAN.3	CSA-High
20 to 24	High	Moderate	AVA_VAN.4	CSA-High
> 24	Beyond High	High	AVA_VAN.5	CSA-High

As the present document only considers the TOE against the Substantial a rating of the CSA the following notes with regards to the role of the evaluator is copied from ETSI TS 102 165-3 [10] and presented in Table 2.

Table 2: Evaluator actions for CSA and attack potential rating

AVA_VAN class	Attack potential	CSA [i.13] rating	Notes
AVA_VAN.1.3E	Basic	Substantial	The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.
AVA_VAN.2.4E			

The mapping to the EAL levels historically used in CC can be found in CC Part 5 [8].

In defining the security functionality of the ONDS management entity the present document fulfils the objectives defined in Article 51 of the CSA [i.13] in combination with the EUCC provisions made in ETSI TS 103 996 [11].

5 The ONDS management TOE

5.1 Introduction

The TOE and the management interface security requirements are defined in ETSI TS 103 961 [1]. The description given in the present document is for information only.

As described in ETSI TS 103 96 [1] the network management manager manages and controls devices on optical networks, supports unified management, and offers control of networks. Thus, the network manager integrates functions including network management, service control, and network analysis. It is an enablement system for network resource pooling, network connection automation and self-optimization, and O&M automation.

5.2 The type of the TOE

The TOE is a software application located on the management and control layer of the cloud-based network. It can manage and control ubiquitous network devices, including transport, IP, and firewall devices. It provides open interfaces to quickly integrate with upper-layer application systems such as OSSs, service orchestrators and service applications. Various apps can be developed and customized to accelerate service innovation and achieve operations.

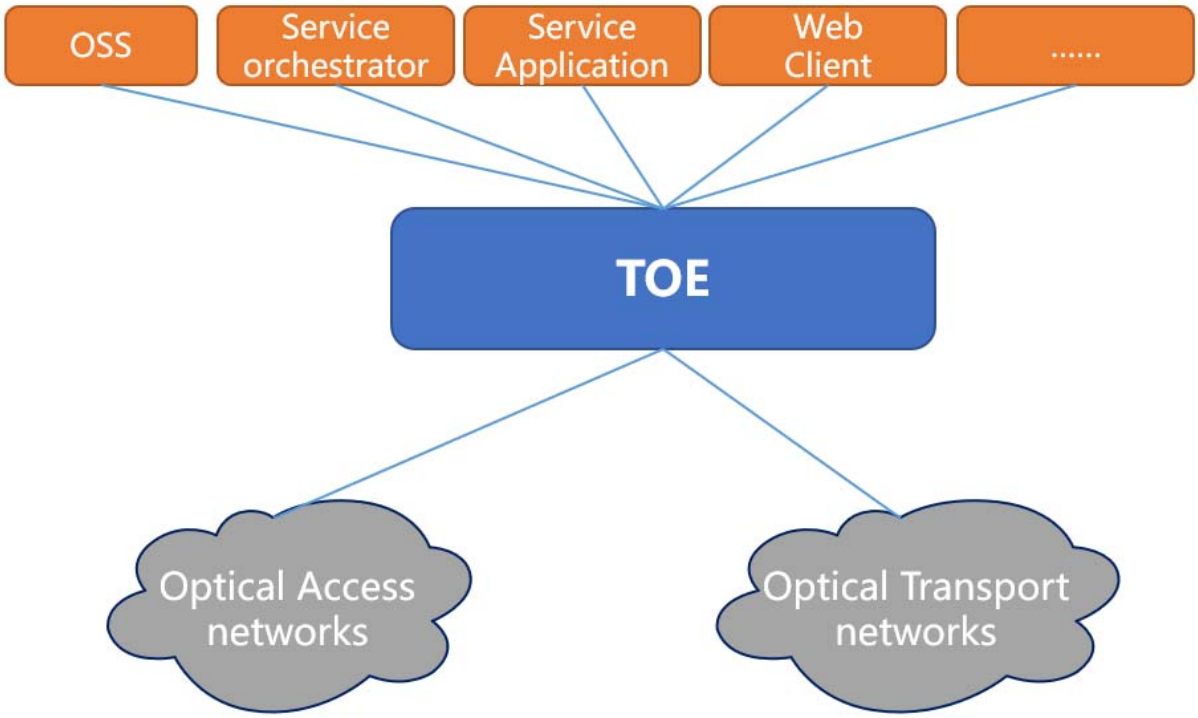

Figure 5: ToE illustration

5.3 TOE Description

The TOE is a single software system located in the management and control layer of the network protecting the assets defined in clause 6.2 against the threats identified in clause 6.4 of the present document.

It is designed to manage and control optical network devices as defined in each of ETSI TS 103 962 [2] and ETSI TS 103 963 [3]. The TOE provides interfaces for integration with upper-layer systems such as OSSs, service orchestrators, and service applications.

The test system requires both the managed device (in the operational network) and in the management centre (as the manager entity) whilst the purpose of the evaluation is to only assess the functionality (described in clause 9 by the SFRs) of the management software as the TOE.

5.4 Main functions and security features of the TOE

The TOE shall support the functions identified in ETSI TS 103 963 [3] that have been identified in order to counter the security threats identified in ETSI TS 103 924 [12]. Thus as identified in ETSI TS 103 961 [1] the following security features are required and are expanded in the present document in the form and style of Common Criteria Security Functional Requirements (CC SFRs) in clauses 8 and 9 of the present document:

- User management
- Identification
- Authentication
- Access control
- Communication security
- Audit
- Security management
- Cryptographic Services

5.5 Physical Scope

Out of scope of the present document.

NOTE 1: The base specifications ETSI TS 103 963 [3] do not define the physical characteristics of the TOE.

NOTE 2: The management functions are wholly software artefacts which rely on certain physical characteristics of the platform to run which are addressed in large part in clause 4 of ETSI TS 103 924 [12].

5.6 Logical Scope of the TOE

5.6.1 User Management

As defined in ETSI TS 103 961 [1], clause 6, the TOE provides access control management to control permissions to users with different responsibilities, and adjusts the permissions based on service changes.

NOTE: The present document extends the role of the manager object defined in ETSI TS 103 961 [1] to the object SMManager that has a role allowing it to create customized user-defined User Groups that may form a class within the access control function.

5.6.2 Authentication and identification

As defined in clause 5 of ETSI TS 103 961 [1], the TOE shall authenticate all entities who access the TOE. The present document extends the definition given in ETSI TS 103 963 [3] to explicitly define, using SFRs in clause 9, the means by which an entity is identified and authenticated.

5.6.3 Access Control

As defined in clause 7.2 of ETSI TS 103 961 [1], the TOE shall support policy based access control.

The present document extends the definition given in ETSI TS 103 963 [3] to explicitly define, using SFRs in clause 9, the means of achieving access control.

5.6.4 Communication security

As defined in clause 6 of ETSI TS 103 961 [1], the TOE shall provide integrity and confidentiality protection of any data in transmission.

5.6.5 Audit

The TOE generates audit records for security-relevant management actions.

NOTE: A Syslog™ as defined in IETF RFC 3164 [i.3], or in the updated IETF RFC 5434 [i.4], solution may be used to resolve the problem of limited storage space.

5.6.6 Security Management

The TOE offers security management for configuration and topology management aspects of the Optical Network. Security management includes not only authentication and access control management, but also management of security-related data consisting of configuration profiles and runtime parameters.

5.6.7 Cryptographic Services

Security functionalities rely and are dependent on the availability of cryptographic services. The TOE provides cryptographic algorithm and key management functions to support secure communication and software update, following endorsed standards, e.g. BSI TR-02102-1 [i.5].

5.7 The non-TOE Components

The following components are out of scope of the present document and not part of the TOE:

- The components of the network device that hosts the TOE.

EXAMPLE 1: The hardware components the TOE is installed on.

- Local and remote management stations operated by the defined administrator user roles to connect to the TOE.

EXAMPLE 2: The Privileged Access Workstation defined in ETSI TS 103 994-1 [i.6] may apply.

- The physical infrastructure interconnecting various network elements. (e.g. cables, switches, etc.)
- Any TOE-host external entity

EXAMPLE 3: Using a Network Time Protocol (NTP) server for synchronizing time for the TOE.

- The operational environment in which the TOE is operated.

5.8 The TOE Lifecycle

Not applicable.

NOTE: In order to be consistent with the aims of the Cyber Resilience Act [i.14] and the NIS2 Directive [i.9] provisions have to be made to ensure that the TOE (the OLT/OTN) has addressed lifecycle and supply chain issues and to be updateable over its lifetime. In this the provisions for vulnerability reporting given in ETSI TS 103 645 [i.8] apply.

6 The Security Problem Definition

6.1 Overview

The security problem which applies to the TOE is described in ETSI TS 103 963 [3] and in the common requirements ETSI TS 103 924 [12]. The text that follows in this clause summarizes the problem statement but the normative text remains in ETSI TS 103 963 [3].

6.2 Assets

The management entity allows managed access to the configuration data of the Optical Network Device (OND) and to the network topology as identified in ETSI TS 103 963 [3]. Each of these assets is identified as having high impact to the network availability if accessed or modified by an unauthorised entity and are thus subject to the suite of access control functions identified in clause 7 of ETSI TS 103 963 [3] and the necessary identification and authentication of the accessing parties as identified in clause 5 of ETSI TS 103 963 [3].

Translating the assets as defined in ETSI TS 103 963 [3] to a CC format is given below.

- D.CONFIG: configuration data of devices and the NMS system itself.

NOTE 1: The ST author may choose to further decompose the configuration data to distinguish configuration data for different operations

EXAMPLE 1: A possible decomposition of the configuration data is to distinguish data for identification, for authentication, for crypto operations and so forth. It is noted however that there is no such decomposition identified in ETSI TS 103 963 [3] where the primary security control is policy based attribute access control.

EXAMPLE 2: Topology data may be part of the configuration data. The topology of the overall system may be inferred from the way in which routing is configured in the configuration data. If the network topology is maintained outside of the management entity (and therefore of the TOE) the topology does not exist as an asset of the TOE, however if the management entity builds a logical network topological map from data obtained by the TOE it is an asset of the TOE.

- A.D.LOG: Audit and log files maintained on the device

In addition are the following secondary assets:

- A.SOFT: The operational software of the management entity (of the OND)
- A.SOFT_UPDATE: An update package for the operational software of the management entity (of the OND)

NOTE 2: The particular operational role of software and the security applied to it may be addressed by other PPs and the relevant PP cited by the ST author.

NOTE 3: The ST author should describe the assets in detail based on the actual application.

6.3 Discussion of the Threats

6.3.1 Overview

In Annex A of ETSI TS 103 961 [1] it is identified that the assets (see clause 6.2) are to be prevented from unauthorised access (see clause 7 of ETSI TS 103 963 [3]) with authorised entities identified and authenticated (see clause 5 of [3]) and data to be maintained as confidential and with integrity verifiable (see clause 6 of [3]).

Translating the threats giving rise to the countermeasures specified in [3] the threats are re-stated in CC format in clauses 6.3.2 through 6.3.4.

6.3.2 T.UnauthenticatedAccess

Unauthenticated entities could manage to bypass the identification, authentication and authorisation and get access to D.LOG and D.CONFIG, perform by that any malicious operation on D.CONFIG, enabling for abusing the TOE for a threat agent's purpose.

6.3.3 T.UnauthorisedAccess

Logged in users with restricted authorisation could manage to escalate their restrictions and access thereby TOE functions that cause compromising of D.LOG and D.CONFIG which enables for any malicious operation and for abusing the TOE for a threat agent's purpose.

6.3.4 T.Eavesdrop

An eavesdropper (remote attacker) in the management network served by the TOE, who is able to intercept, modify, or re-use information assets that are exchanged between the TOE and interconnection party.

6.4 Assumptions

A.PhysicalProtection

The operating environment of the cloud hosting the TOE is protected from unauthorised physical access. Only authorised users have the right to physically access the TOE and its operating environment. The underlying hardware and firmware that host the TOE is trusted and provide the capabilities the TOE requires for correct operation.

Host-external network services the TOE operation requires are always available. The TOE is deployed within a cloud network that is protected from the outer world by the operational environment of the cloud operator.

EXAMPLE: Host-external services the TOE requires for operation can be timestamp-, backup-, or audit servers.

A.NetworkSegregation

Assume that the network interfaces of the server and TOE client are accessible only through the subnet where the TOE host is installed. The subnet is separated from the public network. Communicates with the TOE server through the firewall.

A.AdministratorBehaviour

Any authorised user role is trustworthy, is trained and qualified to operate the assigned functions on the TOE, follows the TOE user guidance, and attempts no adverse or malicious operations on the TOE.

A.Services

The operational environment provides the required services for TOE operations including a reliable time or timestamp source.

A.NetworkElements

The connected NEs and ONDs that are managed by the TOE always use protected communication channels with publicly endorsed standard communication protocols. The channel protection comprises endpoint identification, authentication, integrity and confidentiality protection.

A.Components

Connected TOE-host external NEs, specifically those providing services to the TOE, are effectively protected from being abused and do not adversely or maliciously interact with the TOE.

A.TrustedPlatform

The TOE-host, comprising its HW and its operational SW, is protected against threats that endanger its correct operation. And, this protection is maintained by the cloud operator using state-of-the-art means.

A.RNG

The TOE-host provides a random number service conformant to NIST SP 800-90A [13] with the appropriate entropy quality whenever the TOE requires a random number.

6.5 Security Objectives

O.Authorisation

The TOE shall establish a role model for the authenticated entities where each role receives a set of functions assigned by the security management.

O.Authentication

The TOE identifies and authenticates entities before the authorisation to access TOE resources is granted.

O.Audit

The TOE generates, stores and reviews audit records for security-relevant administrator actions. The audit logs shall be accessible for authorised entities only.

O.Communication

The TOE shall provide protected communication channels, based on publicly endorsed standard protocols, between itself and the connected managed objects. The protection is required to comprise endpoint identification, authentication as well as integrity and confidentiality protection of the transmitted data (that may be used in the policy-based access control defined in ETSI TS 103 963 [3]).

O.SecurityManagement

The TOE shall support the management of its security functions, including as a minimum: access control (as defined in ETSI TS 103 963 [3] but extended to the internal operation of the TOE).

O.Cryptography

The TOE shall operate cryptographic operations as described in Annex A of ETSI TS 103 961 [1] and shall provide mechanisms supporting crypto-agility.

NOTE: The specific algorithms to be maintained are not defined but should follow best practice (e.g. on the basis of publicly endorsed algorithms).

6.6 Security Objectives for the Operational Environment

OE. PhysicalProtection

The operating environment of the cloud hosting the TOE is protected from unauthorised physical access. Only authorised users have the right to physically access the TOE and its operating environment. The underlying hardware and firmware that host the TOE is trusted and provide the capabilities the TOE requires for correct operation. Host-external network services the TOE operation requires are always available. The TOE is deployed within a cloud network that is protected from the outer world by the operational environment of the cloud operator.

EXAMPLE: Host-external services the TOE requires for operation can be timestamp-, backup-, or audit servers.

OE.NetworkSegregation

The operational environment protects the cloud hosting the TOE by separation from other networks. At least a firewall is operated between the TOE-host filter unused communication ports.

The firewall shall be trusted not attack the TOE.

OE.AdministratorBehaviour

Any authorised user role is trustworthy, is trained and qualified to operate the assigned functions on the TOE, follows the TOE user guidance, and attempts no adverse or malicious operations on the TOE.

OE.Services

The operational environment provides the required services for TOE operations including a reliable time or timestamp source.

OE.NetworkElements

The connected NEs and ONDs that are managed by the TOE always use protected communication channels with publicly endorsed standard communication protocols. The channel protection comprises endpoint identification, authentication, integrity and confidentiality protection.

OE.Components

Connected TOE-host external NEs, specifically those providing services to the TOE, are effectively protected from being abused and do not adversely or maliciously interact with the TOE.

OE.TrustedPlatform

The TOE-host, comprising its HW and its operational SW, is protected against threats that endanger its correct operation. And, this protection is maintained by the cloud operator using state-of-the-art means.

OE.RNG

The TOE-host provides a random number service conformant to NIST SP 800-90A [13] with the appropriate entropy quality whenever the TOE requires a random number.

6.7 Security Objectives Rationale

Table 3 provides a mapping of TOE objectives to threats, showing that each objective is at least covered by one threat.

Table 3: Mapping of security objectives to threats

Security Objective for the TOE	Threat
O.Communication	T.Eavesdrop
O.Authentication	T.UnauthenticatedAccess and T.UnauthorisedAccess
O.Authorisation	T.UnauthorisedAccess
O.Audit	T.UnauthorisedAccess and T.UnauthenticatedAccess
O.SecurityManagement	T.UnauthenticatedAccess, T.UnauthorisedAccess and T.Eavesdrop
O.Cryptography	T.Eavesdrop

Table 4 provides a mapping of security objectives for the operational environment to assumptions and threats, showing that each security objective for the operational environment is at least covered by one assumption or threat.

Table 4: Mapping of security objectives for the environment to assumptions and threats

Security Objective for the Operational Environment	Threat / Assumption
OE.PhysicalProtection	A.PhysicalProtection T.UnauthenticatedAccess
OE.NetworkSegregation	A.NetworkSegregation
OE.AdministratorBehaviour	A.AdministratorBehaviour
OE.Services	A.Services
OE.NetworkElements	T.Eavesdrop A.NetworkElements
OE.Components	A.Components
OE.TrustedPlatform	A.TrustedPlatform
OE.RNG	A.RNG

7 Extended Component definition

7.1 SAR SW Update Management

7.1.1 ALC_SWU.1 Software Update Management

The definition of SAR SW Update Management is given in clause 7.1.2.

Recognizing that NMS software may contain vulnerabilities (an exploitable weakness as defined in ETSI TS 102 165-1 [i.1]) and that such vulnerabilities should be mitigated it is necessary to provide a mechanism for maintenance of the software of the device.

NOTE 1: The term patch management is equivalent to other terms including those addressing software update and software maintenance and that give assurance that the software on a device is up to date.

NOTE 2: Software update provisions for devices is addressed in clause 5.3 of ETSI TS 103 645 [i.8] and the present document conforms to the provisions of [i.8] and of the testing of those provisions given in clause 5.3 of ETSI TS 103 701 [i.12] (noting that whilst the scope of the reference documents addresses IoT the functional requirements in the reference documents are universal).

In conformance to the provisions of ETSI TS 103 645 [i.8] and of ETSI TS 103 701 [i.12], the developer shall be able to clearly indicate if software is updateable and the mechanism applied shall pass the tests defined in clause 5.3 of ETSI TS 103 701 [i.12]. This may be assisted by the use of Software Bills of Material (SBOMs), and a clear IXIT (Implementation extra Information for Testing) as defined in ETSI TS 103 701 [i.12].

If an update fails it should be possible for the system to be reverted to a previously known state (noting however that the previous state may contain a known vulnerability).

7.1.2 ALC_SWU.1 Software Update Management

NOTE 1: If developers plan TOE upgrades that impact security functionality of TOE, and the upgraded product retains the same identification, the existing certificate may become invalid and in such cases the certificate should be updated and validation against the latest "good" certificate will apply.

The SW update of the TOE for its security maintenance, in the sense of flaw remediation, corrections in user guidance, and most important for the remediation or mitigation of vulnerabilities. If the TOE update follows the certified update procedures, the TOE update can be done as soon the remediation or mitigation code is available.

The SW update procedures **contain** instructions for secure **signing, distributing, and applying of software updates**.

NOTE 2: None of the information the ST writer may collect to achieve the fulfilment of the SAR ALC_SWU.1 is deemed for the user or the public. This information is to be made available to the evaluator and certification bodies, but to no other party.

Table 5: ALC_SWU.1 Software Update Management

Family name	**ALC_SWU.1 Software Update Management**
Behaviour	This component implements regulation related aspects of the SW patch management.
Levelling	ALC_SWU.1 Software Update Management - 1
Hierarchical to	To no other components.
Management	There are no management activities foreseen.
Dependencies	**ALC_FLR.2**
Audit	There are no actions defined to be auditable.

Dependency

The dependency to ALC_FLR.2 is as a result of the software update management is used as the enabling mechanism for the vulnerability mitigation or remediation. Code that is delivered by the software update management process can serve for mitigation of a vulnerability. In addition, the dependency builds assurance for the flaw remediations, as flaws can also be security flaws inducing vulnerabilities and are resolved using the equal correction procedures.

7.1.3 ALC_SWU.1D Developer action elements

ALC_SWU.1.1D: The developer shall provide the description of the SW update management procedures.

ALC_SWU.1.2D: The developer shall provide security updates based on the defined SW update management procedures at least until the end-of-support period of the TOE has been reached.

Application Note: The ST writer is recommended to define the end of support according to the manufacturer's definition, as that definition may be subject of a regulation affecting the TOE.

ALC_SWU.1.3D: The developer shall provide a protected channel for the download of each update software following the TOE's communication protection capabilities, or, alternatively, provide the patch in secure off-TOE-ways to the user for managing the update.

7.1.4 ALC_SWU.1C Content and presentation elements

ALC_SWU.1.1C: The SW update procedure shall describe the process for the development and release of the patch for the TOE.

ALC_SWU.1.2C: The SW update procedure shall describe the technical mechanism and functions for the adoption of the patch into the TOE.

Application Note 1: That means the description of the TOE mechanism that validates the SW update before it is adopted which means installed.

ALC_SWU.1.3C: The SW update procedure shall describe the mandatory structure and content of the VIAR (Vulnerability Impact Analysis Report).

Application Note 2: The ST writer should consider the requirements of Article 35 of the Implementing Act [12] and the content of Annex IV.3 Changes to a certified product. The VIAR informs the certification body to determine whether a change in view of the developer has a major or minor security impact. The certification body decides then about the certificate maintenance procedures.

ALC_SWU.1.4C: The SW update procedures shall include rules and work items that have to be followed, documented and checked before an update is released.

Application Note 3: The conduct of the SW update procedures shall generate evidence for the evaluation.

ALC_SWU.1.5C: The SW update procedure shall describe the mandatory structure and content of patch release notes.

Application Note 4: A patch release note is user guidance on how to securely operate a specific SW update.

ALC_SWU.1.6C: The SW update procedure shall describe how unfixed flaws are documented.

Application Note 5: Unfixed flaws mean that the developer's risk assessment has decided to accept the risk induced by an identified flaw. The rationale for that decision shall be documented and prove that the evaluation assurance level is not affected.

ALC_SWU.1.7C: The TOE user guidance shall contain a description how the SW update procedure is securely operated.

ALC_SWU.1.8C: The TOE user guidance and the SW update procedure shall enable the user to verify the integrity and authenticity of a SW update.

7.1.5 ALC_SWU.1E Evaluation working units

ALC_SWU.1.1E: The evaluator **shall verify** that the provided information **complies with all requirements** regarding content and evidence presentation.**ALC_SWU.1.2E**: The SW update procedure shall describe a set of evaluation activities related to the effectiveness and performance of the technical mechanism.

Application Note: The ST writer should ensure that the evaluation tests are able to demonstrate the effectiveness of security update functionality of TOE.

8 Additional SFR definitions

Void.

9 Security Functional Requirements

9.1 Overview of SFR hierarchy

NOTE 1: The SFRs in this clause are from CC-Part 2 [5] and, where appropriate, from extensions defined in specifically cited documents. All of the SFRs described are defined with respect to the core requirements from ETSI TS 103 963 [3] and the mapping is summarized in Annex A.

NOTE 2: Where an SFR from CC Part 2 [5] contains the term user, then this is interpreted in a wider sense as any functional entity using another functional entity.

The hierarchy, or dependency tree, for each SFR defined in [5] is explicitly stated in [5] and unless extended or modified by their application in the present document those dependencies shall be followed even if not cited.

EXAMPLE: FAU_GEN.1.2 in [5] is dependent on FPT_STM.1 Reliable time stamps. The present document does not cite the dependent SFR as a distinct requirement.

9.2 Security Audit class (FAU)

9.2.1 FAU_GEN.1 Audit data generation

NOTE 1: The audit class of CC Part 2 [5] supports the requirements of Article 51 c/e/f from the CSA [i.13].

In ETSI TS 103 961 [1] requirements for audit in the event of errors are identified in clause 5, and the detail content of the records is defined in clause 7.3 of [1].

FAU_GEN.1.1 The TSF shall be able to generate audit data of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the ***[selection, choose one of: minimum, basic, detailed, not specified]*** level of audit;

c) **[assignment: other specifically defined auditable events].**

FAU_GEN.1.2 The TSF shall record within the audit data at least the following information:

a) Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;

b) For each auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST, **[assignment: other audit relevant information].**

NOTE 2: The specific data identified by "other audit relevant information", if used and present in the implementation for which an ST is defined, have to be explicitly identified by the ST author.

9.2.2 FAU_GEN.2 User identity association

NOTE: The audit class of CC Part 2 [5] supports the requirements of Article 51 c/e/f from the CSA [i.13].

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

9.2.3 FAU_SAR.1 Audit review

NOTE: The audit class of CC Part 2 [5] supports the requirements of Article 51 c/e/f from the CSA [i.13].

FAU_SAR.1.1 The TSF shall provide **[assignment: authorised users]** with the capability to read **[assignment: list of audit information]** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

9.2.4 FAU_SAR.2 Restricted audit review

NOTE: The audit class of CC Part 2 [5] supports the requirements of Article 51 c/e/f from the CSA [i.13].

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

9.2.5 FAU_SAR.3 Selectable Audit Review

NOTE: The audit class of CC Part 2 [5] supports the requirements of Article 51 c/e/f from the CSA [i.13].

FAU_SAR.3.1 The TSF shall provide the ability to apply **[assignment: methods of selection and/or ordering]** of audit data based on **[assignment: criteria with logical relations]**.

9.2.6 FAU_STG.2 Protected audit data storage

NOTE: The audit class of CC Part 2 [5] supports the requirements of Article 51 c/e/f from the CSA [i.13].

ETSI TS 103 961 [1] requires, in clause 7.3, that both configuration data and the audit trail of changes shall be maintained in a secure store.

FAU_STG.2.1 The TSF shall protect the stored audit data in the audit trail from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to ***[selection, choose one of: prevent, detect]*** unauthorised modifications to the stored audit data in the audit trail.

9.2.7 FAU_STG.4 Action in case of possible audit data loss

NOTE: The audit class of CC Part 2 [5] supports the requirements of Article 51 c/e/f from the CSA [i.13].

FAU_STG.4.1 The TSF shall [**store audit records in the database and export them into files**] if the audit data storage exceeds [**occupies over the default value of 80 % of the database capacity and lasts for over the default duration of 45 days**].

9.3 User data protection

9.3.1 FDP_ACC.1 Subset Access Control

Clause 7.2 of ETSI TS 103 961 [1] defines a number of requirements for access control which are met in part by FDP_ACC.1.

- All data the NMS shall be made available to authorised entities using the principle of least privilege.
- The access control mechanism shall follow the policy model outlined in ETSI TS 102 165-2 [i.5].
- Each protected Object in the OAN device shall be protected by an access control policy
- The access control policy shall be evaluated on each access attempt.

The TSF shall enforce the **access control policy** on **critical subjects and objects** and all operations among subjects and objects covered by the SFP.

NOTE: The critical subjects and objects are those identified in clause 6.2 as configuration data and identities and their associated credentials.

9.3.2 FDP_ACF.1 Security attribute-based access control

NOTE 1: The use of FDP_ACF.1 given below formalizes the access control rules defined in [1] with modifications as required to meet the formatting and wording of the CC SFRs.

FDP_ACF.1.1 The TSF shall enforce the **access control SFP** to objects based on the following:

- **Subject: "User authentication status" with**
  security attribute "Status": "authenticated" or "rejected"
- **Subject: "User role assigned"**
  with security attribute "Role": "Administration user (AU)" or "fail"
- **Object:**
  "TOE resources" with security attributes: "authenticated", "AU"

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects Access is permitted to subjects that are "authenticated" and where the role is AU and the assigned privileges match with the object.**

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **Access and execution to "TOE resources and executable commands" shall only be granted if the "Role" is set to "AU" and the assigned privileges match with the object.**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **Access and execution to the object shall not be granted if its execution requires "Role" being "AU" while the set value is any other value.**

NOTE 2: The assignment of privileges or execution rights to user roles can be subject of the security management FMT_SMF.1 if not defined otherwise.

9.4 Identity and authentication

9.4.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect ***when an administrator configurable positive integer within [assignment: range of acceptable values]*** unsuccessful authentication attempts occur related to **[assignment: list of authentication events]**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***met***, the TSF shall **[assignment: list of actions].**

9.4.2 FIA_ATD.1 User attribute definition

A number of requirements from ETSI TS 103 963 [3] require the mapping of attributes to the NMS for the purpose of authentication, and for the assessment of access control privileges.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: **[assignment: list of security attributes].**

9.4.3 FIA_UAU. 1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow **[assignment: list of TSF mediated actions]** on behalf of the user to be performed before the user is authenticated.

NOTE: In the context of the present document user refers only to an NMS administrator user, i.e. the user managing the protected assets (e.g. configuration data).

FIA_UAU.1.2 The TSF shall require each management user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

9.4.4 FIA_UAU.6 Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the condition **[assignment: list of conditions under which re-authentication is required].**

9.4.5 FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only **[assignment: list of feedback] to** the user while the authentication is in progress.

9.4.6 FIA_UID.1 Timing of identification

In accordance with the least privilege principle, the TSF shall not allow any operational actions by unidentified entities. In addition, as the TSF is mostly deployed without a direct user (i.e. it operates autonomously) the mediated actions shall always be restricted. In this regard therefore, the only actions enabled on the TSF prior to identification and authentication are those required to complete the authentication and authorisation process.

FIA_UID.1.1 The TSF shall allow **[assignment: list of TSF-mediated actions]** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any TSF-mediated actions on behalf of that user.

9.5 Cryptographic Support

9.5.1 FCS_CKM.1 Cryptographic key generation

NOTE 1: As the base requirements from ETSI TS 103 963 [3] do not specify cryptography, the specific wording of assignments in the SFRs from [5] are omitted in the present document, but are expected to be provided in detail in any corresponding ST. The relevant parts are highlighted in clauses 9.5.2 through 9.5.5.

NOTE 2: The specific provision of cryptographic primitives is expected to be paired between participating entities to ensure interoperability.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: cryptographic key generation algorithm]** and specified cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.

9.5.2 FCS_CKM.2 Cryptographic key distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **[assignment: cryptographic key distribution method]** that meets the following: **[assignment: list of standards].**

9.5.3 FCS_CKM.3 Cryptographic key access

FCS_CKM.3.1 The TSF shall perform **[assignment: type of cryptographic key access]** in accordance with a specified cryptographic key access method **[assignment: cryptographic key access method]** that meets the following: **[assignment: list of standards].**

9.5.4 FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.6.1 The TSF shall destroy **[assignment: list of cryptographic keys (including keying material)]** when ***[selection: no longer needed, [assignment: other circumstances for key or keying material destruction]].***

FCS_CKM.6.2 The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method **[assignment: cryptographic key destruction method]** that meets the following: **[assignment: list of standards].**

9.5.5 FCS_COP.1.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[assignment: list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards].**

9.6 Security management class

9.6.1 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:
[assignment:

- **Assignment of privileges and rights to user roles**
- **Management of user accounts**
- **list of management functions to be provided by the TSF**

].

9.6.2 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to ***[selection: determine the behaviour of, disable, enable, modify the behaviour of]*** the functions **[assignment: list of functions]** to **[assignment: the authorised identified roles]**.

9.6.3 FMT_MSA.1 Management of security attributes

The TSF shall enforce the **[assignment: access control SFP(s), information flow control SFP(s)]** to restrict the ability to ***[selection: change_default, query, modify, delete, [assignment: other operations]]*** the security attributes **[assignment: list of security attributes]** to **[assignment: the authorised identified roles]**.

9.6.4 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles **[assignment: the authorised identified roles].**

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

9.6.5 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the **[assignment: access control SFP, information flow control SFP]** to provide ***[selection, choose one of: restrictive, permissive, [assignment: other property]]*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **[assignment: the authorised identified roles]** to specify alternative initial values to override the default values when an object or information is created.

9.6.6 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to ***[selection: change_default, query, modify, delete, clear, [assignment: other operations]]*** the **[assignment: list of TSF data]** to **[assignment: the authorised identified roles]**.

9.7 TOE Access

9.7.1 FTA_TSE.1 TOE Session Establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on **[assignment: attributes]**.

9.7.2 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a **[assignment: time interval of user inactivity]**.

9.7.3 FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

9.7.4 FTA_TAH.1 TOE Access History

FTA_TAH.1.1 Upon successful session establishment, the TSF shall display the ***[selection: date, time, method, location]*** of the last successful session establishment to the user.

FTA_TAH.1.2 Upon successful session establishment, the TSF shall display the ***[selection: date, time, method, location]*** of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.

FTA_TAH.1.3 The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information.

9.8 Trusted Path class

9.8.1 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and ***[selection: remote, local]*** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from ***[selection: modification, disclosure, [assignment: other types of integrity or confidentiality violation]]***.

FTP_TRP.1.2 The TSF shall permit ***[selection: the TSF, local users, remote users]*** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for ***[selection: initial user authentication, [assignment: other services for which trusted path is required]].***

9.8.2 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit ***[selection: the TSF, another trusted IT product]*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **[assignment: list of functions for which a trusted channel is required].**

9.9 Summary of security requirements dependency and rationale

Table 6: Security Requirements Dependency Rationale

Security Functional Requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	Resolved by external time source. The audit time depends on the reliable time stamp. Reliable time stamp depends on external time sources
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.2	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.2	FAU_STG.2
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2 FMT_MSA.3
FIA_UID.1	None	None
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.6	None	None
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2
FIA_ATD.1	None	None
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.2 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FTA_TSE.1	None	None
FTA_SSL.3	None	None
FTA_SSL.4	None	None
FTA_TAH.1	None	None
FTP_TRP.1	None	None
FTP_ITC.1	None	None
FCS_CKM.1	[FCS_CKM.2, or FCS_CKM.5, or FCS_COP.1] [FCS_RBG.1, or FCS_RNG.1] FCS_CKM.6	FCS_COP.1 FCS_RBG.1 FCS_CKM.6
FCS_CKM.2	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1 or FCS_CKM.5] FCS_CKM.3	FDP_ITC.1 FCS_CKM.1 FCS_CKM.3
FCS_CKM.3	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1, or FCS_CKM.5]	FCS_CKM.1
FCS_CKM.6	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1
FCS_COP.1	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1, or FCS_CKM.5] FCS_CKM.6	FCS_CKM.1 FCS_CKM.6

Table 7: Mapping from objectives to SFRs and the rationale to select each SFR

Security objectives	SFR	Rationale
O.Communication	FTP_ITC.1	This SFR ensures the presence of a protected channel that includes identification of the end points as well as confidentiality and integrity protection of the data transmitted.
	FTP_TRP.1	The SFR provides a secure communication channel with external entities through a trusted path, ensuring the confidentiality and integrity of communication data.
	FMT_SMF.1	The SFR finally assigns the attributes to the user role and authorises thereby the user in its roles and manages the rights.
	FCS_CKM.6	Stored and no more used key material could be abused to decrypt previously recorded data at a later point in time. This SFR ensures that those keys are no more present.
		The objective is covered.
O.Authorisation	FDP_ACC.1	Access to management data requires passing the authentication policy this SFR provides. Only successfully authenticated users can access the data.
	FDP_ACF.1	Access to the TOE is only granted when the access control policy was passed which requires the presence of the security attributes meeting the policy rules.
	FIA_UAU.1	This SFR ensures that communication can be initiated from external but else no other action can occur until the user has been authenticated. That ensures that unallowed access to data and resources is not practical.
	FIA_UID.1	This SFR ensures that the TOE first executes on user initiation only actions that serve for authorisation of the user before identification. That ensures that unallowed access to data and resources is not practical.
	FIA_UAU.6	The SFR defines the attributes that are essential for passing the access controls.
	FIA_ATD.1	The SFR defines the attributes that are essential for passing the access controls.
	FMT_SMR.1	This SFR ensures the presence of different user roles that receive in a second step their different access rights respectively privileges. It is a perquisite for the access control policy.
	FMT_MSA.1	Security attributes are critical parameters that should only be set by a specified user role having the privileges to do so. That SFR ensures that only authorised modifications of security parameters are operated.
	FMT_MSA.3	This SFR ensures that right from power on all security attributes come with the correct and secure default values, which can only be set by specified user role have the privileges to do so. Only authorised users can access these data.
	FMT_SMF.1	The SFR finally assigns the attributes to the user role and authorises thereby the user in its roles and manages the rights.
	FIA_AFL.1	This SFR ensures that failed authentications are treated properly and protect from bypassing authentication controls.
		The objective is covered.
O.Authentication	FIA_UID.1	This SFR ensures that the TOE first executes on user initiation only actions that serve for authorisation of the user before identification. That ensures that unallowed access to data and resources is not practical.
	FIA_UAU.1	This SFR ensures that communication can be initiated from external but else no other action can occur until the user has been authenticated. That ensures that unallowed access to data and resources is not practical.
	FIA_UAU.6	This SFR ensures that users need to be re-authenticated at specific time intervals or when a security incident occurs.
	FIA_UAU.7	This SFR ensures that the information fed back to the user during the authentication process does not lead to the leakage of security information.
	FIA_ATD.1	This SFR ensures that failed authentications are treated properly and protect from bypassing authentication controls.
	FIA_AFL.1	This SFR ensures that failed authentications are treated properly and protect from bypassing authentication controls.
	FTA_TSE.1	This SFR ensures that session establishment can be denied based on specific attributes.
	FMT_SMF.1	The SFR finally assigns the attributes to the user role and authorises thereby the user in its roles and manages the rights.

Security objectives	SFR	Rationale
	FTA_SSL.3	A distant entity is out of TOE controls, and an existing but no more used communication channel could be captured. The TOE terminates such connections and protects therewith from abuse of previously authenticated channels.
	FTA_TAH.1	This SFR ensures that a history of successful or failed access attempts to the TOE is provided, enabling authorised users to determine whether there is a risk of their account being misused based on this record.
	FTP_ITC.1	Authentication of users is security critical and related credentials are exchanged. That exchange requires a protected channel between the TOE and the remote entity the user operates.
	FTP_TRP.1	The SFR provides a secure communication channel with external entities through a trusted path, ensuring the confidentiality and integrity of communication data.
		The objective is covered.
O.Audit	FAU_GEN.1	This SFR ensures the logging of security relevant events including defined user (administrator) activities.
	FAU_GEN.2	Ensure that complete audit records are generated, including key information such as event time, subject identity, and event outcome, to provide foundational data for log analysis.
	FIA_UID.1	This SFR ensures that users complete identity verification before performing any operations.
	FAU_SAR.1	This SFR provides the function of accessing security audit records.
	FAU_SAR.2	This SFR restricts unauthorised users from accessing audit information.
	FAU_SAR.3	This SFR provides capability support for authorised users to access the required security audit functions under specified conditions.
	FMT_SMF.1	Control the management and configuration permissions for audit functions to ensure that only authorised personnel can modify log management policies and parameters.
	FAU_STG.2	This SFR prevents audit data from being illegally deleted or modified.
	FAU_STG.4	This SFR defines the measures to be taken when audit record storage exceeds the threshold to prevent loss of audit data.
		The objective is covered.
O.SecurityManagement	FMT_SMF.1	The SFR finally assigns the attributes to the user role and authorises thereby the user in its roles and manages the rights including those for the security functions.
	FIA_ATD.1	The SFR defines the attributes that are essential for passing the access controls and that can be linked with the user role to achieve the correct authorisation.
	FMT_MOF.1	Ensure that only authorised administrators can perform security-related operations and protect administrative data.
	FMT_MTD.1	Ensure that only authorised administrators can perform security-related operations and protect administrative data.
	FMT_MSA.1	Security attributes are critical parameters that should only be set by a specified user role having the privileges to do so. That SFR ensures that only authorised modifications of security parameters are operated.
	FMT_MSA.3	This SFR ensures that right from power on all security attributes come with the correct and secure default values, which can only be set by specified user role have the privileges to do so. Only authorised users can access these data.
	FTA_SSL.4	The TOE provides a mechanism for users to securely terminate their sessions, ensuring that previously authenticated session channels are properly closed and protected from potential abuse.
	FCS_CKM.1	Disclosure protection of intercepted data is achieved with encryption, requiring quality key material of which this SFR ensures the generation.
	FCS_CKM.2	Generated key material has to reach communication entities in secure ways which this SFR ensures.
	FCS_CKM.3	Generated key material has to reach external servers for communication and reception of logging files in secure ways. This SFR ensures that intercepted data remain protected from disclosure.
	FCS_CKM.6	Stored and no more used key material could be abused to decrypt previously recorded data at a later point in time. This SFR ensures that those keys are no more present.
	FCS_COP.1	Provides cryptographic protection mechanisms for secure system operations.
		The objective is covered.

10 SAR Components

10.1 Additional SAR components

10.1.1 SAR SW Patch Management

SAR SW Patch Management is formed to include these aspects into the TOE evaluation in order to verify the correctness of the assigned SFRs and SARs.

SAR Vulnerability processing has been added to the TOE. Passing the evaluation provides the basis for the conformance statement for the assigned SFRs and SARs.

10.1.2 SAR augmentation: ALC_FLR.2 Flaw reporting procedures

NOTE: The CC uses the term "security flaw" where other documentation (e.g. from ETSI) and EU regulation uses the term "security vulnerability". The terms appear to be identical in intent and the broad recommendation in [1] and [2] to adopt the guidance of ETSI TR 103 838 [i.2] and to implement the security controls of ETSI TS 103 305-1 [i.7] apply.

The augmentation with ALC_FLR.2 provides flaw-reporting procedures that require the developer to support the user with corrective actions, and guidance in order to ensure that the user is able to mitigate the discovered flaw.

Table 8: ALC_FLR.2 Flaw reporting procedures

ALC_FLR.2 Flaw Reporting Procedures	
Dependencies:	No dependencies
Developer action elements	
ALC_FLR.2.1D	The developer shall document and provide flaw remediation procedures addressed to TOE developers.
ALC_FLR.2.2D	The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.
ALC_FLR.2.3D	The developer shall provide flaw remediation guidance addressed to TOE users.
Content and presentation elements	
ALC_FLR.2.1C	The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.2.2C	The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
ALC_FLR.2.3C	The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.2.4C	The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.
ALC_FLR.2.5C	The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.
ALC_FLR.2.6C	The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.
ALC_FLR.2.7C	The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.
ALC_FLR.2.8C	The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

10.2 Dependencies of Assurance Components

The writer of any ST conforming to the present document shall consider the inter-dependencies of the SARs as defined in [6] and claimed in clause 4 of the present document with the targeted evaluation assurance level.

Annex A (informative): Mapping between base requirements and SFRs

Table A.1: Mapping between base requirements and SFRs

Item	Requirement text from [3]	Status	Requirement analysis for test and evaluation	Applicable PP SFR (from CC part 2 [5])
Req-1	The provisions for securing the management of the optical network should follow existing best practice for securing management data and protocols	R		NA
Req-2	The overall approach for the security of managed objects of the ON is that the models of least persistence and least privilege shall apply (see NIST SP 800-171)	M	Detail privilege of each role is defined.	FMT_MOF.1 Management of Security Functions Behaviour FMT_MTD.1 Management of TSF Data
Req-3	Each managed object shall create an explicit security association with its managing entity The security association between a managed object and its manager shall give assurance of the following: The identity of participants in the security association, The integrity of data exchanged in the course of the security association, and, The confidentiality of data.	M		FDP_ACC.2 Complete Access Control FDP_ACF.1 Security attribute based access control FMT_SMF.1 Specification of management functions FMT_MSA.1 Management of security attributes FMT_MSA.3 Static attribute initialization FTP_ITC.1 inter-TSF trusted channel FTP_TRP.1 trusted path
Req-4	Within the overall structure the management functions shall be within the management plane, the management plane shall establish the primary trust domain for the entire network. The management plane shall act as the overall root of trust for the relevant operator. The management plane shall establish the trust domain of the operator.	M	Same as Req-3. Define security capability sets for different roles on different planes.	FMT_SMF.1 Specification of management functions FMT_MOF.1 Management of security functions FDP_ACC.2 Complete Access Control FDP_ACF.1 Security attribute based access control FMT_SMF.1 Specification of management functions FMT_MSA.1 Management of security attributes FMT_MSA.3 Static attribute initialization FTP_ITC.1 inter-TSF trusted channel FTP_TRP.1 trusted path
Req-5	Managed entities shall be entered into the trust domain by successfully proving their identity and by validation of the proof of attestation of function to the management plane	M		FIA_UID.1 Timing of identification FDP_ACC.2 Complete Access Control FDP_ACF.1 Security attribute based access control FMT_SMF.1 Specification of management functions FMT_MSA.1 Management of security attributes FMT_MSA.3 Static attribute initialization

Item	Requirement text from [3]	Status	Requirement analysis for test and evaluation	Applicable PP SFR (from CC part 2 [5])
Req-6	Where an entity/device supports multiple independent functions, it shall establish a security and trust association to the primary trust domain for each function	M		FDP_ACC.2 Complete Access Control FDP_ACF.1 Security attribute based access control FMT_SMF.1 Specification of management functions FMT_MSA.1 Management of security attributes FMT_MSA.3 Static attribute initialization FTP_TRP.1 trusted path
Req-7	The management plane shall maintain the security policy for the primary trust domain. The security policy shall be driven from the management plane down to the Optical Network Devices. The managed object should be initialized by the manager object	M		FDP_ACC.2 Complete Access Control FDP_ACF.1 Security attribute based access control FMT_SMF.1 Specification of Management Functions
Req-8	If the managed object detects either loss or corruption of the local configuration file or data it shall request a new set of configuration data from the associated manager. The manager shall ensure that all device configuration data for each managed object is always available.	M	These operations are NE service operations.	NA
Req-9	The optical network manager shall support the following functions: • Discovery and update of the network topology in real time; • Configuration of devices and services; • FCAPS management (Fault Configuration Accounting Performance Security or Fault management, Configuration management, Accounting management, Performance management, Security management); and, • Assurance of network resilience.	M	These operations are NE service operations.	NA
Req-10	The specificities of managing network configuration and performance (e.g. Grade of Service, routing information to indicate where to address/send data, allocation of bandwidth to individual end-points), shall be managed through the configuration data elements	M	These operations are NE service operations.	NA
Req-11	An ON may support multiple services (see Annex D of ETSI TS 103 962 [2]). Each service shall be managed as a discrete managed object (i.e. the service is the managed object).	M	These operations are NE service operations.	NA
Req-12	For the purposes of allowing the manager to make decisions the managed entity shall gather relevant metrics for each of fault management, security breach management, and performance management	M	These operations are NE service operations.	NA
Req-13	ON managers and managed entities shall be identified with both a canonical identity and a semantic identifier. The semantic identifier shall be used to indicate the functional nature of the entity and the attestation of function shall be verifiable by a third party. the attestation of function should be consistent with the Attribute Authority Tree (AAT) model described in ETSI TS 103 486 [i.11]	M		FDP_ACC.1 Subset Access Control FDP_ACF.1 Security Attribute-Based Access Control

Item	Requirement text from [3]	Status	Requirement analysis for test and evaluation	Applicable PP SFR (from CC part 2 [5])
Req-14	All identities shall be cryptographically authenticated	M		FIA_UAU.1 Timing of authentication
Req-15	Where asymmetric encryption is used the canonical identifier shall be asserted using an identity form of public-private key binding (e.g. X.509 identity certificate [i.10])	M		FCS_CKM.1 Cryptographic Key Generation FCS_CKM.2 Cryptographic key distribution FCS_CKM.3 Cryptographic key access FCS_CKM.6 Timing and event of cryptographic key destruction FCS_COP.1 Cryptographic operation
Req-16	Any attribute shall be asserted using an attribute form of public-private key binding (e.g. X.509 attribute certificate [i.10]).	M	No SFR about certificate.	NA
Req-17	Any public key carried in a PKC shall be checked to ensure that it is still valid	M	No SFR about certificate.	NA
Req-18	if the certificate has expired, or if the certificate and its key have been revoked, the verifier shall indicate a certificate verification error	M	No SFR about certificate.	NA
Req-19	if the certificate has expired, or if the certificate and its key have been revoked, the verifier shall not process any data associated to the key	M	No SFR about certificate.	NA
Req-20	In case of failure of the authentication or identification, the time, location and reason for the failure shall be recorded in a log file	M		FIA_AFL.1 Authentication Failure Handling
Req-21	The log file shall only be accessible by the manager object	M		FAU_SAR.1 Audit review
Req-22	Managed objects may be identified using Object Identifiers (OIDs) as attributes of a device. The identity and any associated attributes shall be identified and authenticated within a PKI structure using attribute or identity certificates as appropriate	M	Which managed object?	NA
Req-23	Management functions enabled by a connection between the manager and the managed object should not have persistent security associations between the manager and the managed object	R	Prohibited persistent connection? Only security protocols are displayed.	NA
Req-24	The security association created during the identification and authentication phase should derive a session key used to protect the confidentiality of all data transferred between the manager and the managed object	R		FCS_CKM.1 Cryptographic Key Generation FCS_CKM.2 Cryptographic key distribution FCS_CKM.3 Cryptographic key access FCS_CKM.6 Timing and event of cryptographic key destruction
Req-25	The session key shall be used to encrypt the data using an algorithm agreed in the session establishment	M (Conditional)		FCS_CKM.1 Cryptographic Key Generation FCS_CKM.2 Cryptographic key distribution FCS_CKM.3 Cryptographic key access FCS_CKM.6 Timing and event of cryptographic key destruction
Req-26	To prevent replay the network management system shall support means to protect against replay attacks	M	Using TLS.	FTP_ITC.1 inter-TSF trusted channel

Item	Requirement text from [3]	Status	Requirement analysis for test and evaluation	Applicable PP SFR (from CC part 2 [5])
Req-27	If a persistent shared secret is used as the basis of the session key it shall be randomized using a session-specific variable (e.g. nonce, counter, timestamp) in order to derive the session key	M (C)	No match SFR.	A.RNG
Req-28	It shall not be feasible to determine the value of any shared secret by capture of the session-specific variable or the *en-clair* (plain text) content of the management message	M	No match SFR.	FTP_ITC.1 inter-TSF trusted channel
Req-29	The managed object shall have means to ensure that data in the secure storage area is stored in a form that maintains confidentiality	M	Sensitive information is encrypted and stored using AES.	FCS_COP.1 Cryptographic operation
Req-30	The managed object shall have means to ensure that any data manipulation that leads to loss of data integrity is prevented	M	Use security protocols to ensure integrity.	FTP_TRP.1 Trusted Path
Req-31	The following characteristics shall be met by the secure storage element: Tamper resistant Tamper evident Persistent	M	Use the database to store data and use the database's own capabilities, which is outside the scope of the TOE.	NA
Req-32	If the management system detects any loss of data integrity a security alarm should be raised from the managed object to the associated manager	R		NA
Req-33	The management system shall implement an access control policy in which the right to access any protected element (referred to as objects) shall be made by evaluation of the rules contained in the policy	M		FIA_UAU.6 Re-authenticating
Req-34	The principles of least privilege and least persistence shall apply at all times	M		NA
Req-35	If the manager entity for any managed object changes over time this shall be captured as a policy rule (see ETSI TS 102 165-2 [i.5]) and should be applied with contextual constraints	M		FIA_UAU.1 Timing of authentication
Req-36	If more than one subject (e.g. employee and their manager) is required to authorise a change to a managed object, this shall be addressed in the policy by enforcing at least 2 rules (employee and manager), one for each role, both of which have to pass	M		FIA_UAU.6 Re-authenticating
Req-37	Any change in configuration shall be recorded	M		FAU_GEN.1: Audit data generation FAU_GEN.2 User identity association
Req-38	the record of changes in configuration shall be maintained and stored in a secure storage area (where the key for the secure storage area is managed by an RtS)	M		FAU_STG.1 Protected audit trail storage
Req-39	Read access to log files related to a specific managed object shall be restricted to the related manager and its hierarchy and access control shall be granted as per the roles in the access control policy (additional contextual, identity or role attributes may be added as rules to the policy for evaluation)	M		FAU_SAR.1 Audit review FAU_SAR.2 Restricted audit review FAU_SAR.3 Selectable audit review
Req-40	Irrespectively of where log files are stored the storage shall provide the following security services, where enabled by the manager: proof of integrity of the contents. confidentiality protection of all or part of the content (e.g. in encrypted form)	M		FDP_ACC.1 Subset Access Control

Item	Requirement text from [3]	Status	Requirement analysis for test and evaluation	Applicable PP SFR (from CC part 2 [5])
Req-41	If log files are stored remotely, they shall be transferred in a channel that shall provide the following security services, where enabled by the manager: proof of integrity of the contents; confidentiality protection of the content; and, mutual authentication of the end-points prior to establishment of the transfer channel	M		FTP_ITC.1 inter-TSF trusted channel
Req-42	The period for which log records are to be retained shall be configurable by the manager	M		FAU_STG.3 Action in case of possible audit data loss
Req-43	Any cryptographic provision for ONs shall be crypto-agile	M	Principle. This can be achieved through upgrades, updating.	NA
Req-44	Cryptographic provisions should be designed in such a manner that they are able to support a Quantum Safe approach to both asymmetric and symmetric security	R	Principle. This can be achieved through upgrades, updating.	NA
Req-45	All devices in the ON with a cryptographic function shall ensure that the cryptographic facility is "crypto agile" both within the same class of algorithms, and to allow for migration to an alternative class of algorithm	M	Principle. This can be achieved through upgrades, updating.	NA
Req-46	All algorithms used in ONs should be provisioned as quantum safe, or the underlying mechanisms should be designed as crypto-agile to support a quantum safe algorithm during the life of the equipment and its services	R		NA
Req-47	If passwords are used for authentication the password shall not be stored on the system	M		FIA_UAU.7 Protected authentication feedback
Req-48	If passwords are used the system shall store a cryptographic hash of the password only	M		FCS_COP.1 Cryptographic operation
Req-49	In order to give assurance of a secure connection between 2 entities the entities shall negotiate to support a shared set of algorithms	M		FTP_ITC.1 Inter-TSF trusted channel FTP_TRP.1 Trusted path
Req-50	If an algorithm proposed by the manager is not supported by the managed object, the manager object should raise an exception report indicating the algorithms are unmatched	R	Configuration of trusted channels for connecting to the external entities	FMT_SMF.1 Specification of Management Functions
Req-51	If a decision is made to change the algorithm to one of lower perceived cryptographic strength this should be logged as a potential bid-down attack by the managed object	R	No match SFR. But has the capability to eliminate the prompt when users select weak algorithms.	NA
Req-52	Bid-down attacks should be avoided and if the managed object is not able to support the preferred algorithms of the manager object steps should be taken to update the managed object to support the stronger set of algorithms	R	Belongs to the management action.	NA

Annex B (informative): Mapping to CRA considerations

Table B.1: Mapping for essential requirements of CRA Part 1

Essential Requirements	CC SFR(Substantial) / OE	CC SAR (Substantial)	Rationale
Cybersecurity requirements relating to the properties of products with digital elements	principle, no mapping is required	principle, no explicit mapping is required although the following SARs are identified: ASE_SPD.1 Security problem definition ASE_OBJ.2 Security objectives ASE_REQ.2 Derived security requirements	The definition of the security problem, the security objectives and threats are included in the assurance families ASE_SPD (Security problem definition), ASE_OBJ (Security objectives) and ASE_REQ (Security requirements) (in [CC2022P3]), which define content requirements for the Security Target and their related assessment activities.
(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;		ADV_ARC.1 Security architecture description ADV_TDS.2 Architectural design ALC_CMC.3 Configuration management capabilities – authorised controls ALC_CMS.3 Configuration management scope – Implementation representation CM coverage ADV_TDS.1 or ADV_TDS.2 TDS design	ADV_ARC.1: This SAR provides that the TOE design is based on a clear security architecture ensuring that the security functions meet the desired properties of self-protection, domain separation, and non-bypass ability. The architecture description justifies why the TOE security functionality is complete and all SFRs are enforced. It covers the requirements of the design principles. ALC_CMC.[1/2/3]: This SAR provides a number of requirements ensuring that only authorised, reviewed, managed, controlled, tested and formally accepted components can be made an implemented part of the TOE. ALC_CMS.[1/2/3]: Provides the system that holds and controls the original sources of any piece of code, its identification and also the evidences that led to acceptance. It provides authorised access controls to the configuration list, parts, and implementation representation. Thereby, it assures that modifications were done in "controlled manner with proper authorisations" only. ADV_TDS.1 or ADV_TDS.2: The TOE design description provides information on how the TSF were implemented, the design principles, subsystem behaviour and more, which provides relevant information on the attack surface and therewith risk assessment.

Essential Requirements	CC SFR(Substantial) / OE	CC SAR (Substantial)	Rationale
(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:		APE_REQ Security requirements APE_OBJ Security objectives APE_SPD Security problem description APE_CCL.1 Conformance claims	APE_SPD is the first point in the list as it identifies the risks within the identified operational environment. That provides the basis for the derivation of the objectives which are then fulfilled by the requirements the TOE type has to fulfil. Out of that the CC claim may specify the EAL.
(a) be made available on the market without known exploitable vulnerabilities;		AVA_VAN.2	AVA_VAN.[1/2]: The EUCC "substantial" with AVA_VAN.1 or AVA_VAN.2 ensure the appropriate assurance level for the design, development, production, delivery and maintenance of the TOE. The SAR thereby ensures that the PP consistently meets the security problem definition.
(b) be 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;	FMT_SMF.1 Management of security functions FMT_MSA.3 Static attribute initialization	ADV_ARC.1 Security architecture description	ADV_ARC.1 contains a description how the TSF are securely initialized and protected against tampering FMT_SMF.1 specifies the management functions doing a reset to the defaults. FMT_MSA.3 Static attribute initialization ensures that the default values of security attributes are appropriately either permissive or restrictive in nature.
(c) 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;	FMT_SMF.1 Management of security functions	ALC_FLR.2 Flaw reporting procedures	FMT_SMF.1: Vulnerabilities that occur when the product is in market need to be addressed, among other means, most importantly by security updates. This SFR can and should be used to specifies the management functions or mechanisms for the conduct of the TOE security update. ALC_FLR.[1/2/3]: Flaws and vulnerabilities are handled in equal ways, as flaws in the TOE could be exploited and lead in consequence to vulnerabilities. See also chapter 5.3.3 of ISO/IEC 15408-3 [6]. Both are closely related. The required activities on an incoming or recognized flaw and vulnerability can/are defined by the definition of appropriate procedures implementing the timelines and detailed requirements for tracking and reporting of the applicable regulation, including CRA. ALC_FLR.[1/2/3] ensures that appropriate procedures are in place that meet all the CRA requirements.

Essential Requirements	CC SFR(Substantial) / OE	CC SAR (Substantial)	Rationale
(d) 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;	FIA_UID.1 Timing of identification FIA_UAU.1 Timing of authentication FIA_AFL.1 Authentication failure handling FIA_ATD.1 User attribute definition FMT_SMR.1 Security roles FDP_ACC.1 Subset access control FDP_ACF.1 Security attribute-based access control FAU_GEN.1 Audit data generation		FIA_UID.1 and FIA_UAU.1: to ensure the correct identification and authentication forming the access control. FIA_AFL.1: Access control comprises also the limitation of access attempts that yield no success, in order to avoid brute force or denial of service approaches. The SFR ensures the limitation of attempts and contributes therewith to the access control. FIA_ATD.1: After login, the TOE assigns security attributes to the authenticated entity to further enforce the access control. FDP_ACC.1: This SFR provides the access control policy to control the access to TOE resources. FDP_ACF.1: This SFR implements the access control functions assigned by the security attributes and is linked with FDP_ACC.1. FAU_GEN.1 Audit data generation: the logging enables the administrator to react on failed access attempts in timely manner.
(e) 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;	FDP_ACC.1 Subset access control FTP_ITC.1 Inter-TSF trusted channel FTP_TRP.1 Trusted path		FDP_ACC.1: This SFR provides the access control policy to control the access to TOE resources. FTP_ITC.1: This SFR provides the confidentiality protection of transmitted data within a machine-to-machine communication due to a distinct communication channel with confidentiality and integrity protection. The assured identification of the endpoints provides some additional confidentiality protection, as it prevents an unidentified entity accessing the communication.
(f) 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;	FDP_ACC.1 Subset access control FTP_ITC.1 Inter-TSF trusted channel FTP_TRP.1 Trusted path		FDP_ACC.1: This SFR provides the access control policy to control the access to TOE resources. FTP_ITC.1: This SFR provides the integrity protection of transmitted data within a machine-to-machine communication due to a distinct communication channel with integrity protection.
(g) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (minimization of data);		ADV_ARC.1 Security architecture description	NA (Interpretation by EC JRC and ENISA says it is about GPDR, device does not have any personal data).

Essential Requirements	CC SFR(Substantial) / OE	CC SAR (Substantial)	Rationale
(h) protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;	FTA_SSL.3 Session termination	ADV_ARC.1 Security architecture description	FTA_SSL.3: This SFR contributes to the resilience of the TOE as it prevents from abusing an authenticated but passive session after a time. It could also be linked with FTA_MCS.1. ADV_ARC.1: The architecture description can be used to describe how the TSF protect itself against DoS attacks.
(i) minimize the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;	FAU_GEN.1 Audit data generation	AGD_OPE.1 Operational user guidance ADV_ARC.1 Security architecture description	FAU_GEN.1: This SFR provides the definition of events for reporting which can include the absence of external services that are used for the correct operation of the TSF. The event logging enables the administrator to react and re-establish the missing external service. Thus, this SFR contributes to the fulfilment of the CRA requirement. AGD_OPE.1: The user guidance can provide procedures and advice to preserve reliable external services in order that the TOE does not get restrictions in operation. Also, in dependency when there are no claims for failure handling the user guidance should cover the related aspects. Else, there is a gap, the "negative impact" is not minimized.
(j) be designed, developed and produced to limit attack surfaces, including external interfaces;		ADV_ARC.1 Security architecture description ADV_FSP.3 Functional specification with complete summary AVA_VAN.2 Vulnerability survey ADV_TDS.2 Architectural design	ADV_FSP.[1/2/3]: The functional specification provides a description of the TOE's security functional interfaces which provides relevant information on the attack surface and therewith risk assessment. ADV_TDS.[1/2]: The TOE design description provides information on how the TSF were implemented, the design principles, subsystem behaviour and more, which provides relevant information on the attack surface and therewith risk assessment. ADV_ARC.1: Can demonstrate the consistency of the TOE design with the interface descriptions of the FSP and that there are only interfaces that are essential for TOE operation. ADV_AVA.2: The vulnerability assessment includes penetration testing during which unprotected external interfaces and other vulnerabilities should be discovered.

Essential Requirements	CC SFR(Substantial) / OE	CC SAR (Substantial)	Rationale
(k) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;	FAU_GEN.1 Audit data generation FMT_SMR .1 Security roles	ADV_ARC Security architecture description ADV_TDS.2 Architectural design ADV_FSP.1 Basic functional specification	FAU_GEN.1: This SFR provides the definition of events for reporting which can include occurrence of incidents. The event logging enables the administrator to react and resolve the incident Thus, this SFR contributes to the fulfilment of the CRA requirement. FMT_SMR.1: The threat agent circumventing access controls for identification, still needs to achieve a user role and the assignment of security attributes to be authorised for accessing the corresponding TOE resources. That means that even if he could bypass the identification and authentication controls he still needs to have authorisation to access TOE resources. ADV_ARC.1: The architecture description can be used to describe how the TSF protect itself against tampering and bypassing after an incident occurred. Maintaining the TSF contributes to minimization of the incident's impact. ADV_TDS.2: Describes the design of the TSFI and can describe the mechanisms of how an incident is restricted and limited in its impact. ADV_FSP.1: Describes the link between the access control related SFRs and the TSFIs, so that it can be shown how the SFR prevent in incident to increase in terms of authorization to access TOE resources.
(l) 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;	FAU_GEN.1 Audit data generation FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles		FAU_GEN.1: This SFR provides the definition of events for reporting which can include occurrence of incidents. The event logging enables the administrator to react and resolve the incident Thus, this SFR contributes to the fulfilment of the CRA requirement. FMT_SMF.1 can specify the management functions doing a reset to the defaults, i.e. "factory Reset", which is understood as "opt out" from normal operation with user configuration. FMT_SMR.1 Only certain roles should have the right to opt-out from recording and monitoring.
(m) 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	FCS_CKM.6 Timing and event of cryptographic key destruction	AGD_OPE.1 Operational user guidance ADV_ARC Security architecture description	FCS_CKM.6: This SFR ensures that user generated, or user imported keys are wiped securely when those are no more needed which protects from key disclosure and abuse. AGD_OPE.1: For the case there is no dedicated user accessible secure wiping functions, or a given function of the TOE requires a guidance, the user guidance provides advice and/or procedures to securely wipe the data related to the individual user. ADV_ARC.1: The architecture description can demonstrate that user data and related keys can be securely removed in the context to the "factory reset".

Table B.2: Mapping for essential requirements of CRA Part 2

Essential Requirements	CC SAR(Substanital-EAL3)	Rationale
Manufacturers of products with digital elements shall:	NA	
(1) identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;	"ALC_FLR.2.1D The developer shall document and provide flaw remediation procedures addressed to TOE developers". ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws. ALC_FLR.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws. ALC_FLR.2.5C The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.	(1) is covered with ALC_FLR.2.1D documenting how identified vulnerabilities reach the developer ALC_FLR.2.2D documenting that each flaw is received and handled, ALC_FLR.2.5C shows that user have simple ways to report vulnerabilities to the developer.
(2) in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;	ALC_FLR.2.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users. ALC_FLR.2.6C The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.	(2) is covered when: ALC_FRL.2.4C includes demonstration that there is no undue delay in the conduct ALC_FLR.2.6C when the correction procedures keep security updates separate from functional updates."
(3) apply effective and regular tests and reviews of the security of the product with digital elements;	AVA_VAN.2 Vulnerability analysis covers the required testing. And, regular testing is implicit by the EUCC [i.15] scheme rules.	The EUCC maintenance mechanism implicitly fulfils the requirement, as the EUCC scheme limits a certificate's lifetime, requires reassessment and handles also changes to the TOE.

Essential Requirements	CC SAR(Substanital-EAL3)	Rationale
(4) once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;	ALC_FLR.2.3D The developer shall provide flaw remediation guidance addressed to TOE users. ALC_FLR.2.6C The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users." ALC_FLR.2.8C The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.	(4) is covered as all essential information is disclosed to the users.
(5) put in place and enforce a policy on coordinated vulnerability disclosure;	ALC_FLR.2.3D The developer shall provide flaw remediation guidance addressed to TOE users. ALC_FLR.2.6C The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users	(5) is covered when the procedure description contains a policy for information disclosure.
(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;	ALC_FLR.2: The flaw reporting procedures documentation should comprise the methods to provide flaw information, corrections and guidance on corrective actions	(6) is covered when the procedure documentation of ALC_FLR.2 includes also the information to third parties that provided dependencies to the TOE.

Essential Requirements	CC SAR(Substanital-EAL3)	Rationale
(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner;	ALC_FLR.2.1D The developer shall document and provide flaw remediation procedures addressed to TOE developers. ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws. ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw. ALC_FLR.2.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users."	(7) is covered when ALC_FLR.2.1D demonstrates secure mechanisms for providing updates, ALC_FLR.2.2D ensures that activities are launched for each vulnerability, ALC_FLR.2.2C shows that the status for corrections is tracked which address to achieve the resolution status in a timely manner, ALC_FLR.2.4C details the security means deployed for the methods of provision.
(8) ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.	ALC_FLR.2.3D The developer shall provide flaw remediation guidance addressed to TOE users. ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw. ALC_FLR.2.6C The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users".	(8) is covered when: ALC_FLR.2.3D demonstrates that each update comes with guidance, ALC_FLR.2.2C keeps track of the status including its disclosure to the user ALC_FLR.2.6C shows that users receive the remediation procedures for each update.

Annex C (informative): Bibliography

- ISO/IEC 27001:2022: "Information technology — Security techniques — Information security management systems — Requirements".

History

Version	Date	Status
V1.1.1	January 2026	Publication