ETSI TS 103 996 V1.1.1 (2026-01)

TECHNICAL SPECIFICATION

Cyber Security (CYBER);
EUCC PP for Optical Network and Device Security (ONDS)

Reference
DTS/CYBER-00117

Keywords
cybersecurity, evaluation, testing

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.

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

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.

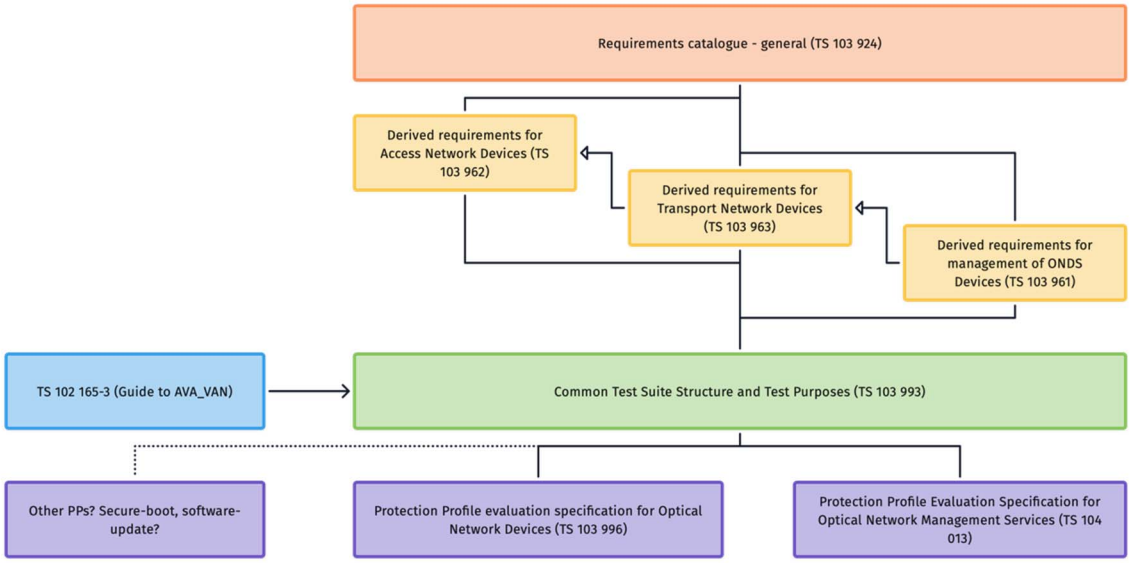


Figure 1: Document structure for Optical Network Device Security

Each of ETSI TS 103 962 [1], ETSI TS 103 963 [2] and ETSI TS 103 961 [i.2] 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 [1] acts as the master document with each of t ETSI TS 103 963 [2] and ETSI TS 103 961 [i.2] 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 [3], 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 [1] and ETSI TS 103 963 [2] in ETSI TS 103 996 (the present document), and to ETSI TS 103 961 [i.2] in ETSI TS 104 013 [i.19].

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 defines the test cases in the form of evaluation criteria and PP/CC evaluation tests resulting from the Test Purposes identified for ETSI TS 103 962 [1] and ETSI TS 103 963 [2] in ETSI TS 103 993 [3]. In combination with the base standard (including its ICS statement), and the TSS&TP in ETSI TS 103 993 [3] this serves as a complete ONDS specification to allow use in the EUCC regime [10] or equivalent under Common Criteria (CC) as a Protection Profile (PP) [4].

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 [10] submission.

NOTE 3: The present document addresses the assurance levels identified in CSA [i.26] for EUCC [10] as Substantial (Article 52.6 of [i.26]).

NOTE 4: In the present document the requirements from ETSI TS 103 962 [1] and ETSI TS 103 963 [2] in the conventional ETSI format are highlighted against the most relevant SFRs from CC-Part 2 [5] in clauses 8 and 9 and in Annex B.

NOTE 5: The present document uses both ETSI style NOTEs that give additional information but are not mandatory, and CC style Application notes that also give additional information but in a more formal way than the ETSI NOTE as an evaluation body is expected to address the content of the application note and to give a justification if the content is ignored.

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 103 962: "CYBER; Optical Network and Device Security; Security provisions in Optical Access Network Devices".

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

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

[4] Common Criteria CCMB-2022-11-001: "Common Criteria for Information Technology, Security Evaluation, Part 1: Introduction and general model", November 2022, Revision 1.

[5] Common Criteria CCMB-2022-11-002: "Common Criteria for Information Technology, Security Evaluation, Part 2: Security functional components", November 2022, Revision 1.

[6] Common Criteria CCMB-2022-11-003: "Common Criteria for Information Technology, Security Evaluation, Part 3: Security assurance components", November 2022, Revision 1.

[7] Common Criteria CCMB-2022-11-004: "Common Criteria for Information Technology, Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities", November 2022, Revision 1.

[8] Common Criteria CCMB-2022-11-005: "Common Criteria for Information Technology, Security Evaluation, Part 5: Pre-defined packages of security requirements", November 2022, Revision 1.

[9] Common Criteria CCMB-2022-11-006: "Common Methodology for Information Technology Security Evaluation, Evaluation Methodology", November 2022, Revision 1.

NOTE: The above listed references ([4] through [9]) are also published by ISO as ISO/IEC 15408 (for [4] through [9]) and as ISO/IEC 18045 (for [8]).

[10] Cybersecurity Certification: Candidate EUCC Scheme V1.1.1.

NOTE: The EUCC scheme is a Common Criteria based European candidate cybersecurity certification scheme and issued by the European Union Agency for Cybersecurity (ENISA).

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

[14] ETSI TS 102 165-2: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures".

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

[i.3] Unified Extensible Firmware Interface (UEFI) Specification Release 2.10.

[i.4] Trusted® Computing Group: "Trusted Platform Module Specification".

NOTE: Available from trusted platform group or as ISO/IEC 11889.

[i.5] ETSI TS 102 165-3: "Cyber Security (CYBER); Methods and Protocols for Security; Part 3: Vulnerability Assessment extension for TVRA".

[i.6] NIST SP 800-133rev2: "Recommendation for Cryptographic Key Generation", June 2020.

[i.7] Recommendation ITU-T X.509: " Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[i.8] NIST FIPS 140-2: "Security Requirements for Cryptographic Modules".

[i.9] NIST SP 800-90B: "Recommendation for the Entropy Sources Used for Random Bit Generation", 2018-01.

[i.10] NIST SP 800-63B: "Digital Identity Guidelines Authentication and Lifecycle Management", 2017-06.

[i.11] ETSI TS 103 994 (V1.1.1): "Cyber Security (CYBER); Privileged Access Workstations; Part 1: Physical Device".

[i.12] ETSI GR NFV-SEC 007: "Network Functions Virtualisation (NFV); Trust; Report on Attestation Technologies and Practices for Secure Deployments".

[i.13] ETSI TR 103 838: "Cyber Security; Guide to Coordinated Vulnerability Disclosure".

[i.14] ETSI TS 103 305-1: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.15] 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.16] ETSI TS 103 701: "Cyber Security (CYBER); Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements".

[i.17] Directive (EU) 2022/2555 of the European Parliament and Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive).

[i.18] ISO/IEC 29147:2018: "Information technology — Security techniques — Vulnerability disclosure".

[i.19] ETSI TS 104 013: "Cyber Security (CYBER); EUCC PP for ONDS management protocols and services".

[i.20] NIST SP 800-164: "Guidelines on Hardware-Rooted Security in Mobile Devices".

[i.21] NIST SP 800-132: "Recommendation for Password-Based Key Derivation Part 1: Storage Applications".

[i.22] Alex Biryukov, Daniel Dinu and Dmitry Khovratovich: "Argon2: the memory-hard function for password hashing and other applications".

[i.23] Tarsnap: "scrypt".

[i.24] ETSI TS 103 486: "CYBER; Identity Management and Discovery for IoT".

[i.25] 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.26] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communication technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[i.27] 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, abbreviations and notation convention

3.1 Terms

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

Administration User (AU): external entity permitted to login to the TOE for the conduct of restricted administration tasks and functionality

NOTE: In a Unix like operational environment this is equivalent to admin.

operational user: autonomous entity that operates the OND

NOTE: In a Unix like operational environment this is equivalent to user.

rogue ONT: ONT that transmits optical signals as upstream at unsynchronized times or time slots that are not assigned to this ONT

sensitive data: data, that if compromised, directly harms the protection and security of the TOE and data operated and resting on the TOE

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.26].

NOTE 2: A mapping from the CSA [i.26] definition to the metrics for risk analysis is given in ETSI TS 102 165-3 [i.5] and in ETSI TS 102 165-1 [i.1].

trusted channel: means by which a Target Of Evaluation (TOE) Security Functionality (TSF) and another trusted IT product can communicate with the necessary confidence

3.2 Symbols

Void.

3.3 Abbreviations

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

APE	Assurance class Protection Profile Evaluation
AU	Administration User
CC	Common Criteria
CIA	Confidentiality, Integrity, Availability
CRA	Cyber Resilience Act
CSA	Cyber Security Act
DoS	Denial of Service
EAL	Evaluation Assurance Level
ENISA	European Union Agency for Cybersecurity
EOL	End Of Life
EUCC	Common Criteria-based European cybersecurity certification scheme
FW	Firmware
HW	Hardware
HWROT	Hardware Root of Trust
ICS	Implementation Conformance Statement
ICT	Information and Communications Technology
ICV	Integrity Check Value
IoT	Internet of Things
IT	Information Technology
IXIT	Implementation eXtra Information for Testing
MAC	Message Authentication Code
NA	Not Applicable
NMS	Network Management System
NTP	Network Time Protocol
OAN	Optical Access Network
OE	Operational Environment
OLT	Optical Line Termination
ON	Optical Network
OND	Optical Network Device
ONDS	Optical Network and Device Security
ONT	Optical Network Termination

OS	Operating System
OTN	Optical Transportation Network
OTP	One Time Programmable
PON	Passive Optical Network
PP	Protection Profile
RTS	Root of Trust for Storage
RTV	Root of Trust for Verification
SAR	Security Assurance Requirement
SBOM	Software Bill Of Materials
SFP	Security Function Policy
SFR	Security Functional Requirement
SFTP	Secure File Tranfer Protocol
SPD	Security Problem Definition
SRU	Service Requesting User
ST	Security Target
SUT	System Under Test
SW	Software
TOE	Target Of Evaluation
TPM	Trusted Platform Module
TSF	TOE Security Functionality
TSS&TP	Test Suite Structure and Test Purposes
TVP	Time Variant Parameter
TVRA	Threat Vulnerability Risk Analysis
VIAR	Vulnerability Impact Analysis Report

3.4 Notation convention for SFRs and SARs

For the purposes of the present document, the notation and structural conventions given in CC-Part 2 [5] and the following 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 CC-Part 2 [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 CC-Part 2 [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 ONDS devices established in ETSI TS 103 962 [1] and ETSI TS 103 963 [2]. 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 (and its normative references, in particular [1], ETSI TS 103 963 [2] and ETSI TS 103 924 [12]) is documented to be consistent with at least Substantial level as defined in the EU Cyber Security Act (CSA) [i.26] and has been designed to be consistent with the requirements of the Common Criteria-based European cybersecurity certification scheme (EUCC) [10].

A PP is defined as an implementation-independent statement of security requirements for a Target Of Evaluation (TOE) addressing a particular type of device (see Common Criteria [4], [5], [6], [7] and [8] (and the corresponding text from ISO/IEC 15408). 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 each of ETSI TS 103 962 [1] and ETSI TS 103 963 [2], and in ETSI TS 103 924 [12].

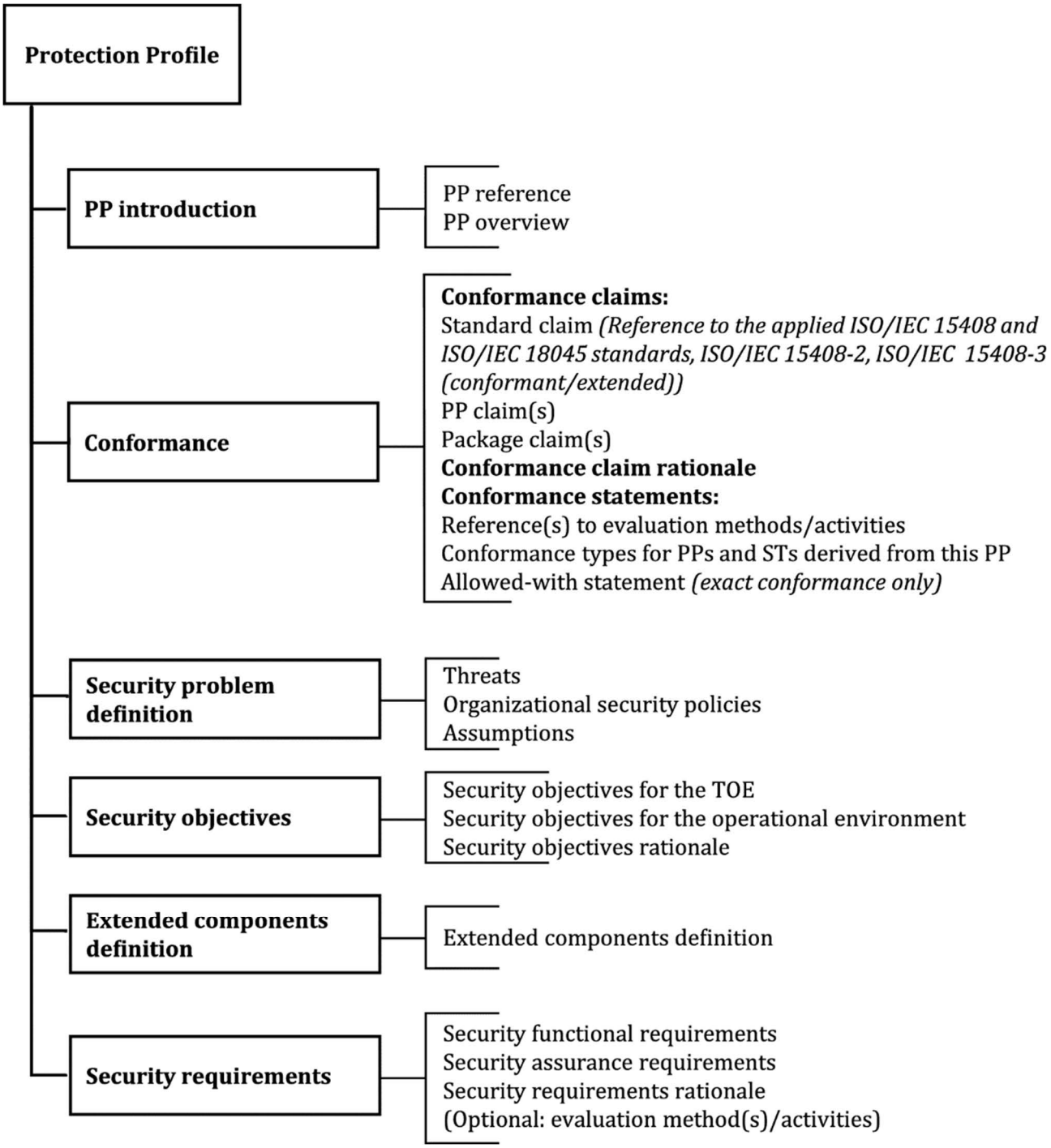
NOTE 2: The term TOE has a similar meaning to System Under Test (SUT) that is conventionally used in ETSI test documents.

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 10 of the present document. In each case the base requirements for ONDS devices established in ETSI TS 103 962 [1] and ETSI TS 103 963 [2] apply, and are mapped to the relevant SFRs in Annex A and to the Test Purposes defined in ETSI TS 103 993 [3] 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 103 962 [1] and ETSI TS 103 963 [2] and ETSI TS 103 993 [3] which is not recommended in CC, although for the present document the ETSI convention is maintained.



NOTE: The figure references ISO/IEC 15408 and ISO/IEC 18045 which are given as alternative sources to those given in clause 2.1 coming from the Common Criteria group [4] to [9].

Figure 2: Contents of a Protection Profile (Source: CC-Part 1 [4], Annex B)

The structure of the PP shown in Figure 1 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 below) 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 1.

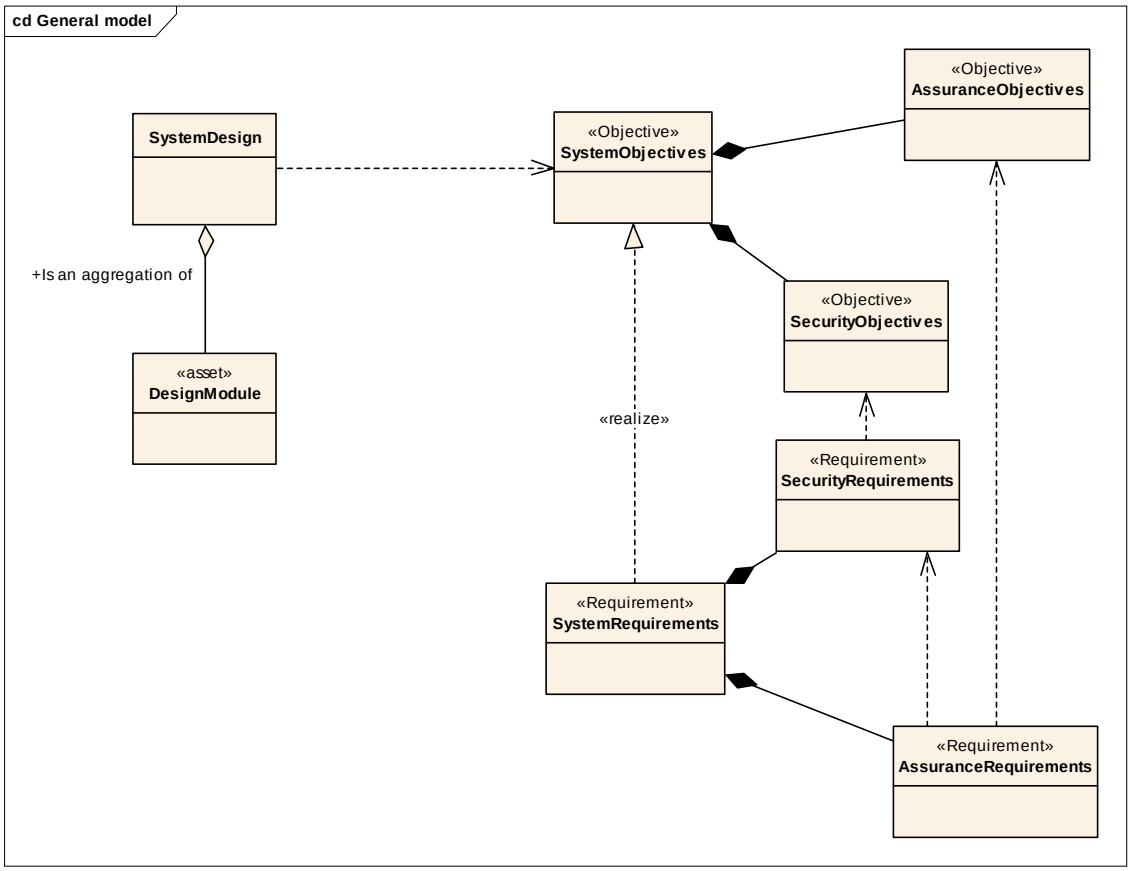


Figure 3: Relationship between system design, objectives and requirements (Source: ETSI TS 102 165-1 [i.1])

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.26] for EUCC [10] as Substantial (Article 52.6 of [i.26]) 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 minimise 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*."

4.1a Conformance claim

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 [5] and [6] as follows:

- CC-Part 2 [5] extended, with FPT_HWROT.1 Root of trust based on HW (see clause 7.1).
- CC-Part 3 [6] extended, ALC_SWU Software Update Management (see clause 7.2).

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

4.2.1 Overview

The present document, including the referenced content of ETSI TS 103 962 [1], ETSI TS 103 963 [2] and ETSI TS 103 924 [12], 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 [10].

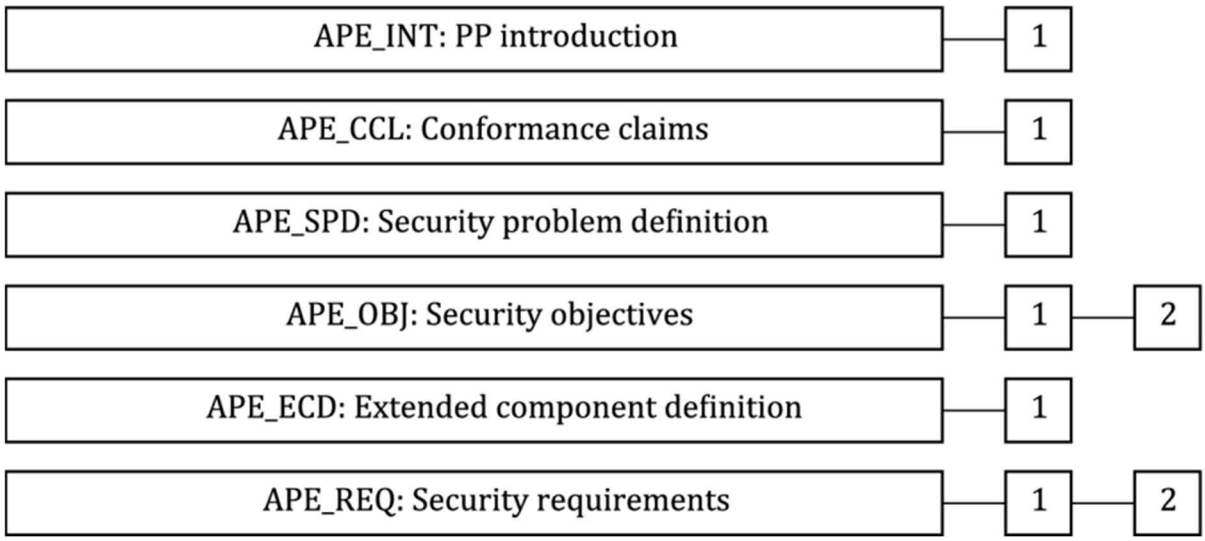


Figure 4: Components of APE class
(Source: CC-Part-3 [6])

4.2.2 Claim against APE_INT

The present document is made with respect to the provisions of ETSI TS 103 962 [1], ETSI TS 103 963 [2] and ETSI TS 103 924 [12].

The unique PP reference (for EUCC [10]) is to the full title and version number of the present document.

ETSI TS 103 996 (V1.1.1): "Cyber Security (CYBER); EUCC PP for Optical Network and Device Security (ONDS)".

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 103 962 [1] and ETSI TS 103 963 [2].

Furthermore, the present PP extends CC-Part 2 [5] with the following SFR extension:

- FPT_HWROT.1 Root of trust based on HW (see clause 7.1)

The chosen Evaluation Assurance Level (EAL) is augmented with ALC_FLR.2, which is defined in CC-Part 3 [6].

The underlying methodology to be considered for the present PP is the CC-Part 3 [6], as applicable to the EUCC programme [10].

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.26].

4.2.4 Claim against APE_SPD

The security problem is defined in the reference documents ETSI TS 103 962 [1], ETSI TS 103 963 [2] and ETSI TS 103 924 [12], 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 103 962 [1], ETSI TS 103 963 [2] and ETSI TS 103 924 [12], and summarized in clauses 6.6 and 6.7 of the present document.

4.2.6 Claim against APE_ECD

The package claim, taken from CC-Part 3 [8] of the present PP is:

EAL3 augmented with ALC_FLR.2

AVA_VAN.2 from CC-Part 3 [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.26] is that AVA_VAN.2 as a minimum is required.

4.2.7 Claim against APE_REQ

The security requirements are defined in the reference documents ETSI TS 103 962 [1], ETSI TS 103 963 [2] and ETSI TS 103 924 [12], 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 [5]). 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.26] 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 [i.5] and presented in Table 2.

Table 2: Evaluator actions for CSA and attack potential rating

AVA_VAN class	Attack potential	CSA [i.26] 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].

5 The ONDS TOE

5.1 Introduction

The TOE is defined in ETSI TS 103 962 [1], ETSI TS 103 963 [2] and by the common requirements in ETSI TS 103 924 [12]. In addition, the management interface security requirements are defined in clause 4 of [i.2] but are out of scope of the present document but are addressed in ETSI TS 104 013 [i.19].

NOTE: The description given in the present document is for information only as the normative definitions are given ETSI TS 103 962 [1], ETSI TS 103 963 [2] and ETSI TS 103 924 [12].

5.2 The type of the TOE

The TOE device provides transparent transmitting services. In this context, transparent means that the TOE does not have the ability to access the data stream contents.

In the optical network scenario, as described in the common requirements catalogue ETSI TS 103 924 [12], and in the specializations of ETSI TS 103 962 [1] and ETSI TS 103 963 [2], there are two types of devices:

- OLT devices connect single Service Requesting Users (SRUs) or user groups that communicate across optical fibre:
  - Multiple SRUs can be grouped and shared on one physical fibre (the security requirements for OLTs are defined in ETSI TS 103 962 [1]).
- OTN devices providing point-to-point transmitting services with the aggregation network and that can manage the OLT traffic (the security requirements for OTNs are defined in clauses 5, 6 and 7 of ETSI TS 103 963 [2]).

Although there are differences between OLT and OTN in network function, both devices can be treated as one TOE type which is covered with the present PP.

5.3 TOE Description

The base requirements given in ETSI TS 103 962 [1] and ETSI TS 103 963 [2] and the common security catalogue in ETSI TS 103 924 [12] apply (see the summary of all requirements given in Annex B of the present document).

5.4 Main functions and security features of the TOE

The base requirements given in ETSI TS 103 962 [1] and ETSI TS 103 963 [2] which come from the common security catalogue in ETSI TS 103 924 [12] apply.

5.5 Physical Scope

Out of scope of the present document.

NOTE 1: The base specifications ETSI TS 103 962 [1], ETSI TS 103 963 [2] and the common catalogue ETSI TS 103 924 [12] do not define the physical characteristics of the TOE.

NOTE 2: The developer of the ST is expected to give a full description of the physical scope of the TOE.

5.6 Logical Scope of the TOE

The base requirements given in ETSI TS 103 962 [1] and ETSI TS 103 963 [2] which come from the common security catalogue in ETSI TS 103 924 [12] apply and address the following characteristics of the TOE:

- Security Management
- Access Control configuration
- Network Management Handling
- TOE Flow Control
- Communication and Cryptographic Services
- Audit & Recovery

5.7 The non-TOE Components

The following components are out of scope of the present TOE:

- The ONDS management components for controlling and administering the TOE (see ETSI TS 103 961 [i.2]).
- The ONDS management component mediating other services that the TOE uses (see ETSI TS 103 961 [i.2]).
- All connecting fibres and wires.
- All radio-equipment, for example Wi-Fi™ and Bluetooth® devices, operated in the TOE environment which interface with the TOE.
- The environment in which TOE is deployed (a guide to environmental provisions is given in ETSI TS 103 924 [12]).

5.8 The TOE Lifecycle

Not applicable.

NOTE: In order to be consistent with the aims of the Cyber Resilience Act [i.26] and the NIS2 Directive [i.17] 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 made in Annex A for software update apply, as do the provisions for vulnerability reporting given in ETSI TS 103 645 [i.15].

6 The Security Problem Definition

6.1 Overview

The security problem which applies to the TOE is described in ETSI TS 103 962 [1] and ETSI TS 103 963 [2] 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 103 962 [1] and ETSI TS 103 963 [2].

The TOE is a managed object where it is configured by the management component [i.2] on behalf of a customer to deliver data to a customer at an agreed grade and quality of service. The TOE has to be able to identify itself to the management component and give assurance to the management component that is has not been compromised. In addition, the management component has to be able to protect itself against malicious attempts to access and modify any configuration data or to its operational software. As the operational software of the TOE is updateable the TOE has to be able to protect itself against any attempt to make unauthorized changes to its software.

NOTE: The nature of the device is that it does not actively interact with the optical data (e.g. explicitly in a Passive Optical Network (PON) and by configuration in any other mode where the device may interact with the signal (e.g. by amplification) but not with the content of the communication).

6.2 Assets

The assets considered in the TOE are described in ETSI TS 103 962 [1] and ETSI TS 103 963 [2] as the configuration data of the device that allows it to perform the actions described above in clause 5.2. The text that follows restates the assets into a format commonly used in CC but the normative definition remains in ETSI TS 103 962 [1] and ETSI TS 103 963 [2].

The security problem identified in ETSI TS 103 924 [12] and formalized as requirements in ETSI TS 103 962 [1] and ETSI TS 103 963 [2] enforce some forms of cryptographic protection of the primary assets of the system. Those primary assets are the configuration data required to make the device operational, and the identifying data required to uniquely identify and connect to the device. The cryptographic protections introduce further assets to the system in the form of keys, algorithms and policies.

In addition, in recognition that the device is software enabled, and that that software is updateable, the software of the device is identified as an asset, protected by access control for both basic operation (i.e. to use the software operationally), and for maintenance (i.e. to allow for the software to be updated).

NOTE 1: In addition to software update the TOE is expected to ensure that the configuration of the software is a protected asset.

The TOE holds and operates assets that require protection against manipulation, disclosure and termination that would endanger the fulfilment of the services the TOE is expected to provide.

The following assets are identified (dependent assets are indicated by formatting as sub-bullets):

- D.ID_CAN: The canonical identifier of the device (see ETSI TS 103 962 [1], ETSI TS 103 963 [2], ETSI TS 103 924 [12]):
  - D.ID_AUTH_CRED: The authentication data (credentials) used to authenticate the identifier.
  - D.ID_AUTH_PROT: The data and protocol used to provide the authentication service.
- D.ID_SEM: The semantic identifier of the device (see ETSI TS 103 962 [1], ETSI TS 103 963 [2], ETSI TS 103 924 [12]).
- D.CONFIG: The configuration data of the device.

NOTE 2: The configuration data is treated as a single asset even if it can be decomposed into discrete configuration data elements.

- D.SOFT: Executable software of the TOE:
  - D.SOFT_UPDATE: The update received by the on-TOE-patch-mechanism, and temporarily stored on the TOE before being installed and activated. It includes executable code, identification (e.g. version and name), and configuration data associated with the patch.

NOTE 3: The D.SOFT_UPDATE asset is dependent on the core asset D.SOFT and is only relevant during an update process (i.e. it is ephemeral and does not exist outside of the update process).

- D.PUBKEY: Public keys and/or certificates on the TOE or retrieved from the HW host to verify the digital signatures of the any received asset, or to decrypt data encrypted with the associated private key.

NOTE 4: The existence of the D.PUBKEY is only required where data verification is required and may be ephemeral or persistent depending on the performance requirement or preference of the device.

- D.AUD_LOG: Audit and log records retained at the device.

6.3 Discussion of the Threats

6.3.1 Overview of threat model

The threat and threat mitigation described in ETSI TS 103 924 [12] and expanded in ETSI TS 103 962 [1] and ETSI TS 103 963 [2] derived the security requirements described in ETSI TS 103 962 [1] and ETSI TS 103 963 [2]. The model used in ETSI TS 103 962 [1] and ETSI TS 103 963 [2] to identify threats is based on the approach given in [i.1] where the textual statement derived from ETSI TS 102 165-1 [i.1] applies: "*A system consists as an aggregation of assets. An asset may be physical, human or logical. Assets in the model may have Weaknesses that may be attacked by Threats. A Threat is enacted by a Threat Agent, and may lead to an Unwanted Incident breaking certain pre-defined security objectives. A Vulnerability is modelled as the combination of a Weakness that can be exploited by one or more Threats. When applied, Countermeasures protect against Threats to Vulnerabilities and reduce the Risk.*" For the purposes of the present document the TOE is the system. A visual representation of the model is given in Figure 5.

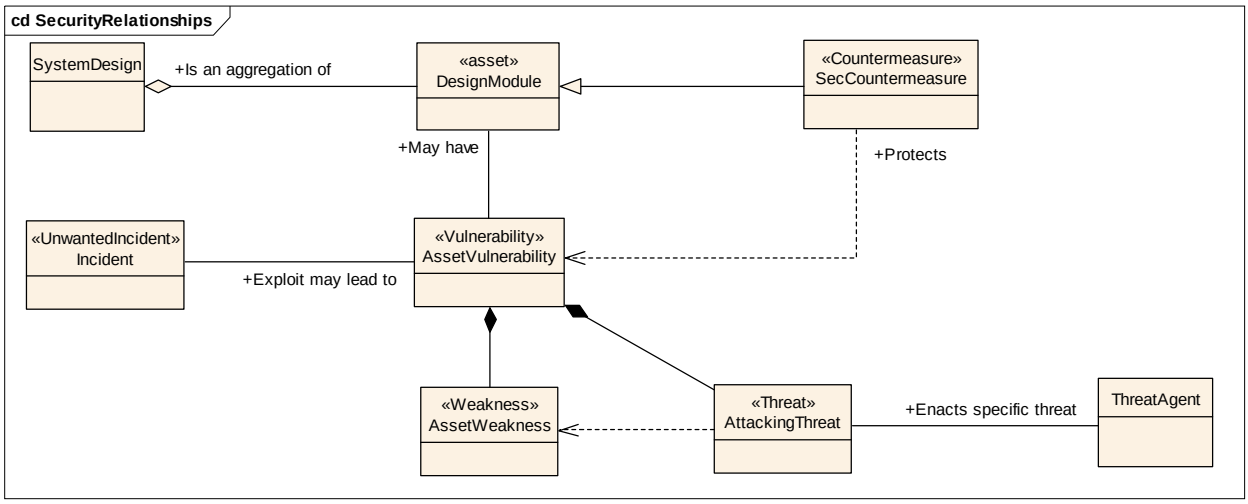


Figure 5: Generic security TVRA model
(Source: ETSI TS 102 165-1 [i.1])

A simplified risk analysis is given in Annex A of the common security requirements in ETSI TS 103 924 [12].

The following text restates the threats in a format commonly used in CC. Threats are identified against the primary CIA attributes as also identified in the threat tree given in ETSI TS 102 165-1 [i.1] as:

- Interception.
- Manipulation.
- Denial of service.
- Repudiation of an action:
  - E.g. Repudiation of change configuration.

For the present document the primary CIA threats identified in ETSI TS 102 165-1 [i.1] as above are restated in CC format below.

T. Repudiation: A threat agent is able to repudiate an action, such as repudiation of modification of configuration of TOE.

- Affected assets: D.AUD_LOG

T.UnauthenticatedAccess: An unauthenticated person may attempt to bypass the security access controls of the TOE to access the TOE as legitimate user.

- Affected assets: D.ID_CAN, D.ID_SEM, D.ID_AUTH_CRED, D.SOFT

T.UnauthorizedAccess: A user with restricted action and information access authorization gains access to unauthorized commands or information. This threat also includes data leakage to non-intended person or device. Discovering unauthorized access in a system with strict access control implies that there has been manipulation of the access control rules, or manipulation of the parameters used to gain access. This threat is the worst scenario, because as an authorized user the threat agent has access and can execute anything. All assets are in danger.

- Affected assets: D.ID_CAN, D.ID_SEM, D.ID_AUTH_CRED, D.CONFIG, D.SOFT, D.SOFT_UPDATE, D.PUBKEY, D.AUD_LOG

The general mapping of threats to system objectives (the CIA triad) are outlined in Table 3.

Table 3: Threats to security objective types
(Source: ETSI TS 102 165-1 [i.1])

Threat	Objective type				
	Confidentiality	**Integrity**	**Availability**	**Authenticity**	**Accountability**
Interception (eavesdropping)	X				
Manipulation - Unauthorized access (note 1)	X	X		X	X
Manipulation - Masquerade (note 2)	X	X		X	X
Manipulation - Forgery (note 3)		X	X	X	X
Manipulation - Loss or corruption of information (note 4)		X	X		
Repudiation		X		X	X
Denial of service			X		
NOTE 1: Unauthorized access in a system with strict access control is taken to imply that there has been manipulation of the access control rules, or manipulation of the parameters used to gain access.					
NOTE 2: Masquerade of an entity as another can be achieved in a number of ways that may include manipulation of data to present an alternative identity.					
NOTE 3: Forgery is a form of manipulation of data to present a false representation (forgery is assumed to be distinct from duplication).					
NOTE 4: Manipulation in its most basic form corrupts data.					

6.3.2 Specific ONDS threats

6.3.2.1 Disclosure of Internal data (T.DiscloseInternalData)

The internal data of the device (the TOE) is its operational software and its configuration data as outlined in clause 6.2 above and noted in the access control rules listed in clause 7.3 of each of ETSI TS 103 962 [1] and ETSI TS 103 963 [2].

NOTE: As any instance of the TOE has a limited degree of personalization (e.g. implementation specific configuration data such as the asset location (virtual or geographical) if present) any compromised device may reveal information that may be used to exploit devices of the same type. The design objectives and development requirements of the device, outlined in ETSI TS 103 924 [12] and captured in part in Annex C, Table C.2 of ETSI TS 103 962 [1] and ETSI TS 103 963 [2], apply.

T.DiscloseInternalData: A threat agent tries to disclose information stored in the TOE and if the TOE has reached its End Of Life (EOL):

- Assumption: Only trained and authorized users can operate the device.

- Objective for the environment: The patch provision system enables the TOE for the verification of the authenticity and integrity of a made available SW patch:

  - Affected assets: D.CONFIG, D.SOFT

6.3.2.2 Misuse of TOE Functions (T.Misuse)

The TOE is intended as a single purpose device (see clauses 4.2 and 4.3 of ETSI TS 103 924 [12]) and is not intended to be used for any other purpose. However, in accepting that the hardware may consist of a computing architecture that is programmable there is a non-trivial risk of the device being misused by inappropriate programming of the TOE functions.

T.Misuse: A threat agent tries to use or abuse the TSF without authorization:

- Affected assets: D. SOFT, D.CONFIG

NOTE: This is normally mitigated by provision of an Access Control mechanism.

6.3.2.3 Interception of communication (T.Intercept)

A number of provisions given in clause 6.1 of ETSI TS 103 924 [12] apply (see also Annex A of each of ETSI TS 103 962 [1] and ETSI TS 103 963 [2]) to protect the content of consumer traffic that is managed by the TOE. As highlighted in clause A.5.1 of ETSI TS 103 924 [12] the application of passive and active measures to detect interference with the physical cable and devices on the cable limit the likelihood of a successful attack, which when combined with the application of encryption to the content (see also the mandates given in clause 6.1 of ETSI TS 103 924 [12]) reduces the risk to a minimum.

T.Intercept: A threat agent tries to intercept the communication between the TOE and external entities to **disclose**, **forge** and **delete** data packets of the communication. A threat agent **records, modifies** and **replays** identification data for reuse at other attack steps:

- Affected assets: D.ID_CAN, D.ID_SEM, D.CONFIG, D.SOFT_UPDATE

NOTE: The conventional mitigation of this threat is by encryption of the communication from the TOE (mitigation against unwanted disclosure) and to give assurance of chronological sequencing of such communication in order to detect deletion, and to give assurance of the integrity of the content of such communication by provision of an integrity verification measure.

EXAMPLE: This threat could arise as a consequence of an inappropriate protocol selection, faulty implementation, or operation with insecure parameters.

6.3.2.4 Tampering with an asset (T.Manipulation)

As identified in the threat taxonomy in ETSI TS 102 165-1 [i.1] tampering is a form of manipulation threat against an asset. Clause 7.1 of ETSI TS 103 962 [1] and ETSI TS 103 963 [2] states that secure storage elements shall be tamper resistant, tamper evident and shall raise an alarm if tampering is identified.

T.Manipulation: A threat agent modifies the configuration data to achieve packet redirections or other perturbations on the traffic A threat agent replays recorded and modified identification data to achieve malfunction or wrong commands of the managing device:

- Affected assets: D.ID_CAN, D.ID_SEM, D.CONFIG

NOTE 1: The conventional mitigation of this form of threat is to provide an integrity verification scheme, such as enabled by cryptographically hashing the data and verification of the hash prior to use where the attacker is unable to generate a valid hash after manipulating the data.

NOTE 2: The mechanism for generating the hash should include a variable parameter (a salt).

6.3.2.5 Malfunction of the TOE (T.Malfunction)

This threat applies to malicious forced malfunction of the TOE.

T.Malfunction: A threat agent tries to cause a malfunction of the TSF in order to deactivate or modify security features or functions of the TOE:

NOTE: Malfunctions of the TOE arising from such things as physical failure of a component are not considered in this PP.

- Affected assets: D.SOFT and D. SOFT_UPDATE and D.CONFIG

EXAMPLE: This could be by sending maliciously crafted data packets, flooding with data packets, or by applying rogue communication.

6.3.2.6 Unauthorized update (T.UNAUTH-UPD)

The TOE shall be updateable to counter threats. This is consistent with requirements identified in the CRA [i.25] and NIS2 [i.17] and is identified as a core requirement in ETSI TS 103 645 [i.15].

T.UNAUTH-UPD: During transmission of a SW patch to the TOE, a threat agent was able to replace or modify the original SW patch with a maliciously crafted SW patch:

- Affected assets: D. SOFT

6.3.2.7 Denial of service by manipulation of update process (T.DOS-UPD)

T.DOS-UPD: A DoS prevents the patch management from operation due to interruption or blocking of the update steps of SW patch loading and/or preventing the atomic conduct of the on-TOE patch mechanism:

- Affected assets: D.SOFT, D.CONFIG

6.3.2.8 Unwanted management traffic (T.UnwantedManagementTraffic)

T.UnwantedManagementTraffic: The traffic here only refers to the traffic on management interfaces, that means, the Unwanted Network Traffic threat only exists on the management plane. The Unwanted network traffic may originate from an attacker and result in an overload of the management interfaces, which may cause a failure of the TOE to respond to system control and normal management operations. As a consequence, the TOE might be unable to provide some of the TSF while under attack and in particular security management functionality to update configuration data for the TOE:

- Affected assets: D.ID_CAN, D.ID_SEM, D.CONFIG, D.SOFT_UPDATE

6.4 Organizational Security Policies

The policy environment in which the TOE is deployed is independent of the device itself thus the examination and definition of organizational security policies is not addressed. Thus no Organization Security Policies (OSPs) are claimed. However, Annex C of ETSI TS 103 962 [1] identifies a number of environmental, deployment, and development constraints to be considered.

6.5 Assumptions

Each of ETSI TS 103 962 [1], ETSI TS 103 963 [2] and the common catalogue ETSI TS 103 924 [12] state a number of assumptions for the use and deployment of the TOE that are re-drafted here into a CC format. The following specifies the assumptions on the TOE environment that are necessary for the TOE to meet its security objectives.

A.Certificates: It is assumed that digital certificates that are generated externally by trusted certification authorities are of good quality i.e. meeting corresponding standards and providing sufficient security strength through the use of appropriate cryptographic mechanisms and cryptographic parameters. This applies for the cryptographic mechanisms and parameters contained in the certificate and as well for the mechanisms and parameters used to sign the certificate. It is assumed that administrators examine the quality of the certificates besides verifying the integrity and authenticity before importing them. Especially certificates signed with weak hashing algorithms are assumed to be not imported into the TOE.

A.PhysicalProtection: It is assumed that the TOE and its operational environment (i.e. the complete system including attached peripherals) are protected against unauthorized physical access. It is assumed that only administrators (i.e. all users who could successfully authenticate to the TOE) are authorized to physically access the TOE and its operational environment. This assumption includes that the management network, including IT trusted products, NMS together with all related communication lines are operated in the same physically secured environment as the TOE.

A.NetworkElements: It is assumed that the operational environment provides securely and correctly working network devices as resources that the TOE needs to cooperate with. Behaviours of such network devices provided by operational environment shall be also secure and correct. These network devices are deployed in an independent network which is segregated from another network.

A.NetworkSegregation: It is assumed that the operational environment provides segregation of networks by deploying the management interface in TOE into an independent local network.

A.NoEvil: It is assumed that personnel working as authorized administrators (i.e. all users that can successfully authenticate to the TOE) shall be carefully selected for trustworthiness and trained for proper operation of the TOE. These administrative users will be competent, and not careless or willfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.Monitoring: It is assumed that the network management systems or administrators continuously monitor the TOE operation for occurring failures and misbehaviours, and, if so, appropriate resolution and mitigation means are executed to restore the normal functioning of the TOE.

A.Device: It is assumed that the underlying hardware of the optical network device, which is outside the scope of the TOE, as well as the firmware and the underlying OS and non-TOE software, are trusted and work correctly.

6.6 Security Objectives

The security objectives resulting in the mitigations given in ETSI TS 103 962 [1] and ETSI TS 103 963 [2] are based on the common catalogue ETSI TS 103 924 [12]. The text that follows restates those objectives into a format commonly found in CC part 1 [4], chapter 10.6.2.

O.CONF_01: The content of a transmission should not be available to an attacker even if the raw data is intercepted.

NOTE 1: This objective is met by the mandates given in clause 6.1 of ETSI TS 103 924 [12].

NOTE 2: The matching objective of not making management and control data available to an attacker is addressed in [i.19] and by O.AVAIL_02.

O.AVAIL_01: Endpoints of each link should be uniquely identifiable, and should be able to verify their identity.

NOTE 3: This objective is met by the mandates given in clause 5.1 (for canonical identifiers) and in clause 5.2 (for semantic or functional identifiers) of ETSI TS 103 924 [12].

O.AVAIL_02: Data (content, control, signalling) that is essential to the management of the network should only be visible to authorized entities in the network.

NOTE 4: This objective is met by the mandates given in each of clauses 7.3 and 7.4 of ETSI TS 103 924 [12].

O.DataFilter: The TOE shall ensure that only allowed management traffic goes through the TOE.

O.Authentication: The TOE shall authenticate users before access to data and security functions is granted.

NOTE 5: This objective is stated in clause 5.2 of ETSI TS 103 924 [12].

O.Authorization: The TOE shall implement different authorization roles that can be assigned to users in order to restrict the functionality that is available to them.

O.Audit: The TOE shall provide functionality generate audit records for security-relevant administrator actions.

O.Communication: The TOE shall implement logical protection means to ensure integrity and confidentiality for network communication between the TOE and Network Management System (NMS) as well as the TOE and trusted IT products from the operational environment.

NOTE 6: This objective includes the requirements identified in clauses 6.1 and 7.2 of ETSI TS 103 924 [12].

O.SecurityManagement: The TOE shall provide functionality to manage security functions provided by the TOE.

NOTE 7: This objective is stated in clause 4.4 of ETSI TS 103 924 [12].

O.SWVerification: The TOE shall provide functionality to allow code loading only when it was prior successfully verified in terms of authenticity and integrity.

NOTE 8: This objective includes updates and patches from external entities.

NOTE 9: The extended assurance requirement for Software Update described and defined in Annex A of the present document applies to this objective.

6.7 Security Objectives for the Operational Environment

Each of ETSI TS 103 962 [1], ETSI TS 103 963 [2] and the common catalogue ETSI TS 103 924 [12] define requirements for the operational environment and are redrafted here in a CC format. See in particular Annex B and Annex C of ETSI TS 103 962 [1] and ETSI TS 103 963 [2].

OE.Certificates: Digital certificates that are generated externally by trusted certification authorities shall be of good quality i.e. meeting corresponding standards and providing sufficient security strength through the use of appropriate cryptographic mechanisms and cryptographic parameters. This applies for the cryptographic mechanisms and parameters contained in the certificate and as well for the mechanisms and parameters used to sign the certificate. Administrators shall examine the quality of the certificates besides verifying the integrity and authenticity before importing them. Especially certificates signed with weak hashing algorithms shall not be imported into the TOE.

OE.PhysicalProtection: The TOE and its operational environment (i.e. the complete system including attached peripherals) shall be protected against unauthorized physical access. Only authorized users have the right to physically access the TOE and its operating environment.

The management network, including the RADIUS server, syslog server, NTP server, SFTP server together with all related communication lines shall be operated in the same physically secured environment as the TOE. Network Management System (NMS) shall be physically protected on the same level as the TOE but they do not necessarily have to be kept in the same physical environment. The communication lines between any trusted IT products (including NMS) and the TOE are protected by cryptographic means and do not need any physical protection. The NMS as well as trusted IT products e.g. RADIUS server, NTP server, SFTP server or syslog server, shall be connected to the TOE via the same segregated management network (see also OE.NetworkSegregation). As a result, the TOE and its operational environment shall be physically protected and shall not be subject to physical attacks.

OE.NetworkElements: The operational environment shall provide securely and correctly working network devices as resources that the TOE needs to cooperate with. The behaviour of such network devices provided by the operational environment shall be secure and correct. This applies to NMS and Trust IT products.

OE.NetworkSegregation: The operational environment shall provide segregation of networks by deploying the management interface in TOE into an independent local network.

OE.NoEvil: Personnel working as authorized administrators (i.e. all users that can successfully authenticate to the TOE) shall be carefully selected for trustworthiness and trained for proper operation of the TOE. These administrative users shall be competent, and not careless or wilfully negligent or hostile, and shall follow and abide by the instructions provided by the TOE documentation. All user management and permission management are implemented in the TOE.

OE.Monitoring: The network management systems continuously monitor the TOE operation for occurring failures and misbehaviours, and, if so, appropriate resolution and mitigation means are executed to restore the normal.

OE.Device: The devices or servers connecting and interacting with the TOE, as well as all the media, e.g. a copper wire, fibre or radio interfaces, used for this communication, shall operate correctly.

6.8 Rationale for Security Objectives

Table 4 demonstrates that all threats are countered with the assigned objectives for the TOE and the Operational Environment (OE).

Table 4: Rationale for security objectives

Threat / OSP	Security Objectives	Rationale for Security Objectives
T.UnauthenticatedAccess	O.Authentication O.Audit O.AVAIL_01 O.SecurityManagement	The threat of unauthenticated access to the TOE is countered by requiring the TOE to implement an authentication mechanism for its users, (O.Authentication). The unique identification of endpoints and identity verification prevents that unknown entities could maliciously access a connection, (O.AVAIL_01). Authentication mechanisms as well as account management can be configured by users with sufficient user level, (O.SecurityManagement). In addition, login attempts are logged allowing detection of attempts and possibly tracing of attack, (O.Audit).
T.UnauthorizedAccess	O.Authorization O.AVAIL_02 O.SecurityManagement O.Audit	The threat of unauthorized access is countered by requiring the TOE to implement an access control mechanism, (O.Authorization). Management data on the network are separated from other data and are only visible to authorized users, (O.AVAIL_02). Access control mechanisms (including user levels) can be configured by users with the corresponding user role and related authorization, (O.SecurityManagement). In addition, actions are logged allowing detection of attempts and possibly tracing of culprits, (O.Audit).
T.Intercept	OE.NetworkSegregation O. Authentication O.AVAIL_01 O. Authorization O. Communication O.CONF_01	First the network segregation ensures that the management traffic between TOE and NMS is unlike to be intercepted. (OE.NetworkSegregation). The authentication means ensure that only NMS administrator can access the TOE. (O.Authentication). The unique identification of endpoints and identity verification prevents that unknown entities could maliciously access a connection. (O.AVAIL_01). Furthermore, each authenticated user receives authorization rights according to their role which is limited to what is needed (managed) (O.Authorization). The logical protection means deployed by the communication in protocol ensure that the data remain integrity and confidentiality protected. (O.Communication and O.CONF_01).
T.UnwantedManagementTraffic	O.DataFilter O.SecurityManagement OE.NetworkSegregation	This threat is countered by O.DataFilter ensuring that unwanted traffic is filtered and cannot deplete the network resources. The filter rules can be configured by authorized users with sufficient user level (O.SecurityManagement). An independent local network is used to manage the TOE. (OE.NetworkSegregation).
T.DiscloseInternalData	O.Authentication O.Authorization	Internal data requires identification and authentication to achieve access and the user role, O.Authentication. Logged in user authorization ensures that only the permitted and authorized user can access internal data, O.Authorization.
T.Misuse	O.SWVerification O.Authorization	This prevents from misuse, as only authentic, integrity checked and if applicable with the correct version can be loaded, O.SWVerification. Logged in user authorization ensures that only the permitted and authorized user can access internal data, O.Authorization.

Threat / OSP	Security Objectives	Rationale for Security Objectives
T.Manipulation	O.Communication O.AVAIL_01	Data in transit can be lost or falsified which is prevented O.Communication. Identity verification of the endpoints ensure that data are exchanged between identified endpoints only, O.AVAIL_01.
T.Malfunction	OE.Monitoring	The occurrence of failures and misbehaviour need to be detected and resolved by the network management centre.
T.Repudiation	O. Authentication O. Authorization O.Communication	Only authorized and authenticated users are allowed to modify the configuration of the TOE, and any corresponding actions such as modifications or deletions shall be audited. (O. Authentication, O. Authorization) Only authorized and authenticated users are permitted to access log files. The logical protection means deployed by the communication protocol ensure secure synchronization of log files between trust IT product and TOE, (O.Communication).
T.UNAUTH-UPD	O.SWVerfication	This ensures that only authentic, integrity verified, and correctly received patches can be installed.
T.DOS-UPD	OE.NetworkElements OE.NetworkSegregation	Patching and update provision occurs on the management network with trusted NE devices only, OE.NetworkElements renders a DOS attack to not practical. The network segregation ensures that patches use the segregated management network. OE.NetworkSegregation renders a DOS attack to not practical.

6.9 Rationale for Objectives for the Environment

Table 5 provides a mapping of the objectives for the operational environment to assumptions, showing that each environmental objective is covered exactly by one assumption. The objectives for the environment are mirrored by the assumptions:

- A.Certificates is upheld by OE.Certificates, which is a rephrasing of the assumption.
- A.PhysicalProtection is upheld by OE.PhysicalProtection, which is a rephrasing of the assumption.
- A.NetworkElements is upheld by OE.NetworkElements, which is a rephrasing of the assumption.
- A.NetworkSegregation is upheld by OE.NetworkSegregation, which is a rephrasing of the assumption.
- A.NoEvil is upheld by OE.NoEvil, which is a rephrasing of the assumption.
- A.Monitoring is upheld be OE.Monitoring, which is a rephrasing of the assumption.
- A.Device is upheld by OE.Device, which is a rephrasing of the assumption.

Table 5: Mapping objectives for the environment to assumptions

Environmental Objective	Threat /Assumption
OE.Certificates	A.Certificates
OE.PhysicalProtection	A.PhysicalProtection
OE.NetworkElements	A.NetworkElements
OE.NetworkSegregation	A.NetworkSegregation T.UnwantedManagementTraffic
OE.NoEvil	A.NoEvil
OE.Monitoring	A.Monitoring
OE.Device	A.Device

7 Extended Component definition

7.1 FPT_HWROT.1 Root of Trust based on hardware

As identified in Table 6 a number of requirements from ETSI TS 103 962 [1] and ETSI TS 103 963 [2] explicitly call out for a hardware based root of trust within the computing platform of the TOE. There are multiple variants of the root of trust identified as below:

- Root of Trust for Storage (RTS) - this shall provide a protected repository and a protected interface to store and manage keying material (i.e. Public Keys and Public Key Certificates, symmetric keys and their related security association records).
- Root of Trust for Verification (RTV) - this shall provide a cryptographic accelerator to verify digital signatures associated with software/firmware and create assertions based on the results.
- Policy Enforcement Engine - to enforce the capabilities described by the ON Device Configuration Record.

The requirements cited in Table 6 are used to inform the selection of SFRs that support a hardware root of trust.

Table 6: Requirements from ETSI TS 103 962 [1] and ETSI TS 103 963 [2] supporting a hardware root of trust

Item	Requirement	Status
Req-1	An OAN device shall consist of at least 1 (one) execution environment.	M
Req-2	An OAN device's execution environment shall have 1 (one) initial root of trust.	M
Req-3	The execution environment shall have at least one executable code block.	M
Req-4	There should be a discrete execution environment for each side and discrete roots of trust for each side.	R
Req-5	If an OAN device supports a multi-occupancy client environment it shall provide confidentiality services at the client side to ensure physical and cryptographic separation of distinct clients.	M C
Req-6	The OAN Device shall have a root of trust used for initialization to enable secure boot capabilities.	M
Req-7	The OAN Device shall implement a root of trust where the scope of functions enabled by the root of trust shall be defined in succeeding clauses of the present document.	M
Req-8	The guidelines given in NIST SP 800-164 [i.20] shall be followed in order to provide the following local (device specific) trust services: Root of Trust for Storage (RTS); Root of Trust for Verification (RTV); Policy Enforcement Engine.	M
Req-9	The manufacturer of the OAN Device shall attest to the provision of the root of trust by reference to the method applied.	M
Req-10	The manufacturer of the OAN Device shall publish the attestation of the provision of the root of trust in the technical specification of the OAN Device.	M
Req-11	The presence of the hardware root of trust shall be asserted by a platform specific attribute certificate.	M
Req-12	The OAN device shall have a root of trust for storage to store private cryptographic material (private key).	M
Req-13	Every access device shall have a Root of trust for Storage (RtS).	M
Req-14	For an access device there should be independent RtSs for the user/client side and for the network side of the device.	R

Clause 7.1 of ETSI TS 103 924 [12], and clause 4.3 of ETSI TS 103 962 [1] state requirements for the provision of a root of trust. As stated in clause 4.3 of ETSI TS 103 962 [1] the manufacturer of the OAN Device shall attest to the provision of the root of trust by reference to the method applied (e.g. a TCG standard TPM or equivalent module [i.4]) and shall publish that attestation in the technical specification of the OAN Device. In addition, as identified in the definition for root of trust in NIST SP 800-164 [i.20], the presence of the hardware root of trust shall be asserted by a platform specific attribute certificate.

The present document extends the provisions in ETSI TS 103 962 [1] and ETSI TS 103 963 [2] by identification of the extended component FPT_HWROT.1.

Rationale: The root of trust based on hardware, HWROT, ensures that a device launches the boot process only when it has confirmed the validity and correctness of the present code. The execution of the 'secure boot' process ensures that any software running on the device is authenticated and has verified integrity.

NOTE 1: This extended component protects the boot process and ensures that the TSF are initiated correctly.

NOTE 2: As the component protects the suite of TSFs the component belongs to the protection of the TSF class.

Behaviour: This family defines the requirement for the presence of a root of trust implemented as immutable HW based module for hosting TSF and other sensitive data.

Levelling:

Hierarchical to: No other component.

Management: There are no management actions foreseen.

Dependencies: This family has no dependencies.

Audit: There are no actions defined to be auditable.

FPT_HWROT.1.1: The TSF shall contain an immutable root of trust that contains trusted data

[selection, choose one of: certificate, public key, hash of public key/s, hash of certificates, [assignment: other credential values]],

which are preserved in:

[selection:

- ***a. a one-time-programmable (OTP) memory,***
- ***b. a dedicated security component,***
- ***c. [assignment: other HW components]***

7.2 Extended SAR components

7.2.1 SAR SW Update Management

7.2.1.1 ALC_SWU.1 Software Update Management general principles

NOTE 1: See also Annex A.

The definition of SAR SW Update Management is given below.

Recognizing that software enabled devices 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 2: 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 3: Software update provisions for devices is addressed in clause 5.3 of ETSI TS 103 645 [i.15] and the present document conforms to the provisions of [i.15] and of the testing of those provisions given in clause 5.3 of TS 103 701 [i.16] (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.15] and of ETSI TS 103 701 [i.16] 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.16]. This may be assisted by the use of Software Bills of Material (SBOMs), and a clear IXIT as defined in ETSI TS 103 701 [i.16].

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) (see the provisions for rollback given in clause A.3.2).

7.2.1.2 ALC_SWU.1 Software Update Management functionality and behaviour

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 7

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.

7.2.1.3 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.

7.2.1.4 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 Vulnerability Impact Analysis Report (VIAR).

Application note 2:
The ST writer should consider the requirements of Article 35 of the Implementing Act [i.27] 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.

7.2.1.5 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 any tests cited are able to demonstrate the effectiveness of security update functionality of TOE.

7.2.2 Add-on for AGD_OPE.1.4C Operational User Guidance

Application note for AGD_OPE.1.4C.
The SAR AGD_OPE.1.4C requires the operational user guidance to present each security-relevant event relative to the user role and function that need to be performed. It needs to be ensured that these user presentations comprise also the case of the TOE decommissioning.

7.2.3 SAR augmentation: ALC_FLR.2 Flaw reporting procedures

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.

Application note 1:

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 ETSI TS 103 962 [1] and ETSI TS 103 963 [2] to adopt the guidance of ETSI TR 103 838 [i.13] and to implement the security controls of ETSI TS 103 305-1 [i.14] apply.

Application note 2:

A vendor may choose to implement the guidance given in ISO/IEC 29147 [i.18] or other standards as an alternative to the recommendations given in ETSI TS 103 962 [1] and ETSI TS 103 963 [2]. If this path is selected it has to be made clear which process for flaw or vulnerability reporting is undertaken.

Application note 3:

In most cases the liability for mitigation is the developer or provider and not the end user, the end user is expected (see for example ETSI TS 103 645 [i.15]) to be able to implement the mitigation without undue effort.

Application note 4:

The essential requirements of the CRA [i.25] in Article 14 requires that the manufacturer reports vulnerabilities to the common reporting platform described in Article 16 of the CRA [i.25] and the manufacturer is expected to address those requirements from the CRA in the implementation of the procedures identified in the present document.

Table 8

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.

8 Security Functional Requirements

8.1 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 103 962 [1] and ETSI TS 103 963 [2] and the mapping is summarized in Annex B.

NOTE 2: Where the term user is used in the SFRs from CC Part 2 [5] it is given the wider interpretation for the present document of any functional entity making use of another functional entity.

The hierarchy, or dependency tree, for each SFR is explicitly stated in [5]. Table 9 summarizes the dependencies of each SFR in the present document (where CC-Part 2 [5] identifies a list of optional dependencies Table 9 identifies the dependencies that have been identified as relevant to the present document).

Table 9: Security Requirements Dependency Rationale

Security Functional Requirement	Dependency	Resolution
FAU_GEN.1	FPT_STM.1	The TOE relies on the external NTP server to provide the timestamp.
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] FCS_CKM.3 Cryptographic key access [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction	FCS_CKM.2 FCS_COP.1 FCS_CKM.3 FCS_RNG.1 FCS_CKM.6
FCS_CKM.2	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access	FDP_ITC.1 FCS_CKM.1 FCS_CKM.3
FCS_CKM.3	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation or FCS_CKM.5 Cryptographic key derivation]	FDP_ITC.1 FCS_CKM.1
FCS_CKM.6	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	FDP_ITC.1 FCS_CKM.1
FCS_COP.1.1	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access	FDP_ITC.1 FCS_CKM.1 FCS_CKM.3
FCS_RNG.1	No dependencies.	Not applicable
FDP_ACC.1	FDP_ACF.1 Security attribute-based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute	FDP_ACC.1 FMT_MSA.3
FDP_SDC.1	No dependencies.	Not applicable
FDP_SDI.1	FCS_COP.1	FCS_COP.1.
FIA_AFL.1	FIA_UAU.1 Timing of authentication	FIA_UAU.1
FIA_API.1	No dependencies	Not applicable
FIA_ATD.1	No dependencies	Not applicable
FIA_UAU.1	FIA_UID.1 Timing of identification	FIA_UID.1
FIA_UID.1	No dependencies	Not applicable
FMT_MSA.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.1
FMT_SMF.1	No dependencies	Not applicable
FPT_INI.1	No dependencies	Not applicable
FPT_STM.1	No dependencies	Not applicable
FTA_SSL.3	FMT_SMR.1 Security roles	FMT_SMR.1
FTP_ITC.1	No dependencies	Not applicable
FPT_HWROT.1	No dependencies	Not applicable

8.2 Security Audit class (FAU)

8.2.1 FAU_GEN.1 Audit data generation

NOTE 1: In the context of ETSI TS 103 962 [1] and ETSI TS 103 963 [2] the term log or logging is used to refer to data gathered in the context of certain system actions for use in the conduct of further enquiry, including audits, whereas in CC-Part 2 [5] the term audit is used to include the gathering of data that is later audited or subject to examination. In the present document logs and audit records are treated as the same.

NOTE 2: The requirements stated in Annex C, Table C.3 of ETSI TS 103 962 [1] and ETSI TS 103 963 [2] apply in addition to those listed in this clause and apply to the wider environment in which the TOE is deployed

The base specifications ETSI TS 103 962 [1] and ETSI TS 103 963 [2] identify conditions for making a log record, and the associated content of the log record, in Requirements 76, 77 and 80:

- Every denied access attempt shall be recorded.
- The record of each denied access attempt shall include at least the following: subject-identifier; object-identifier; date/time of failed access attempt; logical and (if available) physical location of the object; if available the logical and physical location of the subject.
- If an exception is raised it shall include the details of the rule that failed.

These core requirements are translated to the following SFRs defined in CC-Part 2 [5]:

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 detailed level of audit; and

c) the following specific events:

1) Attempts to update FW- and/or SW parts of the TOE, including the update result and final status.

2) Any attempt to access or modify the log record.

3) TOE management and configuration activities by the management entity.

NOTE 3: Item (a) in FAU_GEN.1.1 is required to ensure that a record is maintained of any period in which auditing/logging is switched off.

As defined in Requirements 76, 77 and 80 from ETSI TS 103 962 [1] and ETSI TS 103 963 [2] the log records shall be detailed as shown below. This is reflected in the following SFR from CC-Part 2 [5].

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]**.

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

NOTE 4: It is recommended that the ST author considers the twelve monitoring and logging requirements of NIS2 [i.17], chapter 3.2 to which the operator of the network is obligated, and which the TOE may support.

8.3 Cryptographic Support

8.3.1 FCS_CKM.1 Cryptographic key generation

NOTE 1: As the base requirements from ETSI TS 103 962 [1] and ETSI TS 103 963 [2] do not specify the cryptographic algorithms or key sizes specific wording of assignments in the SFRs from CC-Part 2 [5] are omitted in the present document but are expected to be provided in detail in any corresponding ST.

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

NOTE 3: The references to key in the requirements below are to be read as meaning cryptographic key.

The base requirements from ETSI TS 103 962 [1] and ETSI TS 103 963 [2] do not specify cryptographic algorithms or key sizes, but rather refer to best practice in Annex D of ETSI TS 103 924 [12]. Thus whilst FCS_CKM.1.1 applies in general the details of the cryptographic provisions shall be supplied by the Security Target claiming compliance to the present document. For the purpose of evaluation and assessment of a pass verdict of Requirements 24, 41 and 52 from ETSI TS 103 962 [1] and ETSI TS 103 963 [2] (see also Annex B) the provisions of NIST SP 800-133rev2 [i.6] should be taken into account.

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]**.

8.3.2 FCS_CKM.2 Cryptographic key distribution

The base documents ETSI TS 103 962 [1] and ETSI TS 103 963 [2] only specify key distribution in the context of exchange of public key material for signature verification (Requirement 52, see Annex B). In conventional practice a public key and its association to an attribute is distributed using a Public Key Certificate in the context of a Public Key Infrastructure. In such cases the provisions of Recommendation ITU-T X.509 [i.7] should be taken into account. Thus whilst FCS_CKM.2 applies in general the specific details should be completed by the ST developer.

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]**.

8.3.3 FCS_CKM.3 Cryptographic key access

Whilst the base documents ETSI TS 103 962 [1] and ETSI TS 103 963 [2] do not specify the use of specific cryptographic material they do suggest from Annex A of ETSI TS 103 924 [12] that best practice is followed wherein keys are only made available to the function requiring them and are not available by any other mechanism.

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]**.

8.3.4 FCS_CKM.6 Timing and event of cryptographic key destruction

Whilst the base documents ETSI TS 103 962 [1] and ETSI TS 103 963 [2] do not specify the time at which cryptographic keys are destroyed, but cite both best practice (in ETSI TS 103 924 [12]) and least persistence as guiding principles, the primary requirement is Requirement 41 from ETSI TS 103 962 [1] and ETSI TS 103 963 [2] that states that the association of a key is removed when the association is closed. This shall be taken to imply that key material for each association is ephemeral (but may be derived from a persistent key) and shall, for the purposes of the present document, be interpreted for FCS_CKM.6 as below.

NOTE 1: The base documents ETSI TS 103 962 [1] and ETSI TS 103 963 [2] do not explicitly define any keys hence it is not possible to list keys or keying material in the SFR.

FCS_CKM.6.1: The TSF shall destroy **[assignment: list of cryptographic keys (including keying material)]** when ***no longer needed***.

NOTE 2: The base documents ETSI TS 103 962 [1] and ETSI TS 103 963 [2] do not explicitly define any special storage for ephemeral keys hence for the present document only means to destroy persistent keys at end of service are considered.

FCS_CKM.6.2: The TSF shall destroy **persistent** 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]**.

8.3.5 FCS_COP.1 Cryptographic operation

The base requirements from ETSI TS 103 962 [1] and ETSI TS 103 963 [2] identify a number of cryptographic operations in support of system and data integrity including the generation and verification of Integrity Check Values using hashing or Message Authentication Code algorithms, and digital signatures.

In particular Requirements 62, 63, 64 and 65 from ETSI TS 103 962 [1] and ETSI TS 103 963 [2] apply which identify the scope and timing of operations (including actions on failure):

- All exchanged discrete messages shall have their integrity verified on reception at the device.
- The integrity check function shall be cryptographically strong and may be included in a MAC for symmetric keyed associations, or in a digital signature for asymmetric keyed associations.
- Any message that fails the integrity check shall be discarded and an error reported.
- In order to mitigate against replay attacks a Time Variant Parameter (TVP) should be included with the plaintext prior to calculation of the Integrity Check Value (ICV).

The evaluator shall verify that the ST conforming to the present document expands and explicitly defines the assignments for each SFR.

FCS_COP.1.1: 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]**.

8.3.6 FCS_RNG.1 Random number generation

For the generation of random numbers as defined in ETSI TS 103 962 [1] and ETSI TS 103 963 [2] the FCS class shall apply with the restrictions identified below consistent with requirements stated in [1] and ETSI TS 103 963 [2].

FCS_RNG.1.1: The TSF shall provide a **physical or non-physical-true or deterministic** random number generator that implements: **[assignment list of security capabilities]**.

NOTE 1: The use of software-only random number generators is explicitly disallowed by Requirement 46 from ETSI TS 103 962 [1] and ETSI TS 103 963 [2], however, this does allow for the use of deterministic RNGs where additional requirements are stated as for FCS_RNG_EXT.1.2 below (see also Annex A).

FCS_RNG.1.2: The TSF shall provide **random numbers that meet [assignment: a defined quality metric]**.

NOTE 2: The metrics for random number generation are specified in clause 5 of ETSI TS 103 924 [12].

NOTE 3: If an equivalent standardized definition of random number generation is used then the ST has to explicitly identify it.

EXAMPLE: The requirements described in Annex C of FIPS 140-2 [i.8] and using the model of non-determinism from NIST SP 800-90B [i.9] may be applied.

8.4 User data protection

8.4.1 Summary of requirements for user data protection

The core requirements for accessing data of the TOE are rooted in the least-privilege and least-persistence paradigms that underpin most cybersecurity provisions.

Specific access control rules are specified in Requirement 82 of ETSI TS 103 962 [1] and ETSI TS 103 963 [2] Strict conformance tests of the access control policy are suggested in the TSS&TP [3].

8.4.2 FDP_ACC.1 Subset Access Control

Requirements 71, 72, 73 and 74 from ETSI TS 103 962 [1] and ETSI TS 103 963 [2] apply and are met in part by FDP_ACC.1:

- All data in OAN devices shall be made available to authorized entities using the principle of least privilege.
- The access control mechanism shall follow the policy model outlined in ETSI TS 102 165-2 [14].
- 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.

FDP_ACC.1.1: 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.

8.4.3 FDP_ACF.1 Security attribute based access control

As noted above the access control model defined in clause 7 of each of ETSI TS 103 962 [1] and ETSI TS 103 963 [2] is a Policy and Attribute Based Access Control model. Each of ETSI TS 103 962 [1] and ETSI TS 103 963 [2] identifies specific rules to be implemented by the access control mechanism.

In addition, on the principle of least privilege required by clause 7.2 of ETSI TS 103 962 [1] and of ETSI TS 103 963 [2] the default access control condition shall be DENY, thus satisfying FDP_ACF.1.4 from CC-Part 2 [5].

FDP_ACF.1.1: The TSF shall enforce the **[assignment: access control SFP]** to objects based on the following: **[assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]**.

FDP_ACF.1.2: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]**.

FDP_ACF.1.3: The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]**.

FDP_ACF.1.4: The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]**.

NOTE 1: The specific wording in ETSI TS 103 962 [1] and ETSI TS 103 963 [2] is "do not allow"/"do not permit" which is interpreted for the present document as DENY.

NOTE 2: See also clause A.3 for access control requirements related to Software Update.

8.4.4 FDP_SDC.1 Stored data confidentiality

FDP_SDC.1.1: The TSF shall ensure the confidentiality **of all sensitive user data** while it is stored in persistent memory.

NOTE: Where user data includes a password that password should be stored in a manner that is consistent with clause 5.1.1 of NIST SP 800-63B [i.10] to provide resistance to offline attacks.

EXAMPLE: Algorithms identified to provide such resistance include password hashing schemes an outline of which is given in ETSI TS 102 165-2 [14] and which may be implemented using algorithms such as PBKDF2 [i.21], Argon2 [i.22] or scrypt [i.23].

8.4.5 FDP_SDI.1 Stored data integrity monitoring

Clause 6.1 of ETSI TS 103 962 [1] identifies a number of requirements for establishing and verifying the integrity of data received by or transmitted from the TOE. The additional requirement here is consistent with the post reception (or pre-transmission) of data where that data comes from a data store on the TOE and is therefore consistent with the general provisions for stored data given in clause 7.1 of ETSI TS 103 962 [1].

FDP_SDI.1.1: The TSF shall monitor sensitive user data stored in containers controlled by the TSF for integrity errors on all objects, based on the following attributes: [**assignment: user data attributes**].

NOTE: All user data stored in containers can be TSF data and needs to be protected.

8.5 Identity and authentication

8.5.1 FIA_AFL.1 Authentication failure handling

With respect to the general principle of least privilege and to Requirement 78 of ETSI TS 103 962 [1] and ETSI TS 103 963 [2] the following SFRs from CC-Part 2 [5] apply. In particular, the error reporting threshold shall be defined by the ST and the evaluator shall ensure that a policy exists to address the functionality of the device when the threshold is reached.

EXAMPLE: If the error-reporting threshold is met the device may deny any further access for a fixed period of time.

FIA_AFL.1.1: The TSF shall detect when ***an administrator configurable positive integer (Error-reporting-threshold)*** unsuccessful authentication attempts occur related to **failed access control attempts**.

NOTE 1: The constant "Error-reporting-threshold" is outlined (but not explicitly named as such) in clause 4.5 and also in clause 7.2 of each of ETSI TS 103 962 [1] and ETSI TS 103 963 [2].

FIA_AFL.1.2: When the defined number of unsuccessful authentication attempts has been ***met***, the TSF shall **raise an exception report and deny access according to the local policy**.

NOTE 2: The general model for raising of an error or exception report at the TOE is described in clause 4.5 of ETSI TS 103 962 [1].

8.5.2 FIA_API.1 Authentication proof of identity

Proof of identity of any claimant shall be achieved by an appropriate authentication protocol (see also FIA_UAU.1 in clause 8.5.4 below). Each instance where an entity (as claimant) requires to be identified shall indicate the specific method of how authentication shall be achieved.

FIA-API.1: The TSF shall provide an [**assignment: *authentication mechanism***] to prove the identity of [**assignment: *entity***] by including the following properties [**assignment: *list of properties***] to an external entity.

As FIA-API.1 may be invoked or applied multiple times in the TOE there may be multiple variants of the text of FIA_API.1. There shall only be one authentication mechanism defined and made available for each authentication instance.

There are a number of authentication mechanisms cited in ETSI TS 103 962 [1] and ETSI TS 103 963 [2] that apply depending on circumstance, including challenge-response protocols, Message Authentication Codes (MACs) and digital signatures. Only one authentication mechanism shall apply for each security association. If a simple username-password combination is used it should only be used in such a manner that the password is not revealed in plaintext form and should be used only if no stronger method (i.e. cryptographically valid) is available or practicable and the ST writer should make it clear why the provisions of this clause cannot be satisfied.

8.5.3 FIA_ATD.1 User attribute definition

A number of requirements from ETSI TS 103 962 [1] and ETSI TS 103 963 [2] require the mapping of attributes to the device for the purpose of authentication, and for the assessment of access control privileges. Whilst not explicit in ETSI TS 103 962 ETSI TS 103 962 [1] and ETSI TS 103 963 [2] it is assumed that where attributes are maintained in the context of a public key infrastructure and the exchange of public key certificates that the attributes defined, in for example Recommendation X.509 [i.7], apply and are consistent with the provisions of the cited SFR from CC-Part 2 [5] given below.

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

- **User identification credentials**
- **User authentication credentials**
- **User level**
- **Security attributes specified by FMT_SMF.1 and mapped to the user level by FMT_MSA.1**
- **[assignment: list of security attributes]**

8.5.4 FIA_UAU.1 Timing of authentication

In support of the principle of least privilege, all entities seeking an action from another entity shall be identified and authenticated, and their right to the requested action shall be verified. This is stated in clause 5 of ETSI TS 103 962 [1] and ETSI TS 103 963 [2] and captured in Requirements 3 and 30 from ETSI TS 103 962 [1] and ETSI TS 103 963 [2] and reflected in the following SFR from CC-Part 2 [5].

FIA_UAU.1.1: The TSF shall allow ***no TSF mediated actions*** on behalf of the user to be performed before the user is authenticated.

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

NOTE: In the context of the present document the overall principle of least privilege applies and only authenticated users are allowed access to functions and data.

8.5.5 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 authorization process. The general provisions to be met are identified in clause 5.1 of ETSI TS 103 962 [1] and ETSI TS 103 963 [2].

FIA_UID.1.1: The TSF shall allow **[assignment: *only actions that are necessary to prove authorization*]** 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.

NOTE: Clause 5.1 of ETSI TS 103 962 [1] and ETSI TS 103 963 [2] suggests the use of an Authentication-Session-Time-Limit variable to manage the principle of least persistence in order to ensure that authenticated sessions are strictly time limited.

8.6 Security management class

8.6.1 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1: The TSF shall enforce the **Access Control Policy** 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 authorized identified roles]**.

8.6.2 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1: The TSF shall enforce the **Access Control Policy** 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 authorized identified roles]** to specify alternative initial values to override the default values when an object or information is created.

8.6.3 FMT_SMR.1 Security roles

There is no user role as such in the TOE, rather the TOE operates autonomously as a low privilege device. The autonomous operation shall be defined with respect to a least privilege user. All restricted, non-operational actions, for example, modification of configuration data, are subject to the access control policy. It may be reasonable to simplify the access control rules by assignment of roles (an access control rule may then be classed as a PASS if the role is matched).

Where roles are used in the access control policy or its rules the following apply.

FMT_SMR.1.1: The TSF shall maintain the roles:

- **Administration User (AU): an external entity permitted to access the TOE for the conduct of restricted administration tasks and functionality.**
- **Operational user: A user with restricted permission and assigned administration tasks and functionalities.**

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

8.6.4 FMT_SMF.1 Specification of Management Functions

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

a) **Accounts, roles and rights management**

b) **Audit**

c) **TOE operation management**

d) **Management of credentials and keys**

e) **SW update functionality**

f) ***[Selection: none, or list of [further management functions]]***

NOTE: See also clause A.3 for discussion of the role of FMT_SMF.1 related to software update functionality.

8.7 Protection of the TSF class

8.7.1 FPT_INI.1 TSF initialization

Whilst not strictly addressed in the base specifications ETSI TS 103 962 [1] and [2] the following requirements extend from the assumption that the TSF/OND as a device has to be securely initialized. The further assumption is that the code and data required to start and initialize the device is verified before use.

NOTE: The facilities of the Unified Extensible Firmware Interface (UEFI) industry standard [i.3] which includes a Secure Boot feature to implement boot integrity may be applied in parallel to the use of an industry standard Trusted Platform Module (TPM) [i.4] to implement secure initialization of the TSF/OND.

FPT_INI.1.1: The TOE shall provide an initialization function which is self-protected for integrity and authenticity.

FPT_INI.1.2: The TOE initialization function shall ensure that certain properties hold on certain elements immediately before establishing the TSF in a secure initial state, as specified in Table 10.

Table 10: FPT_INI.1.2 Table

ID	Properties	Elements
1	Integrity	[***selection, choose one of: certificate, public key, hash of public key, hash of certificates, [assignment: other credential values***]]
2	**[assignment: property, for instance authenticity, integrity, correct version]**	**[assignment: list of TSF/user firmware, software or data]**

FPT_INI.1.3: The TOE initialization function shall detect and respond to errors and failures during initialization such that the TOE ***[selection: is halted, successfully completes initialization with [selection: reduced functionality, signalling of error state, achievement of secure state, [assignment: list of actions]]***.

FPT_INI.1.4: The TOE initialization function shall only interact with the TSF in data loading method during initialization.

The following extended requirements apply to any TSF data loading method:

- The operation of loading of TSF data shall be non-interruptible.
- During the TSF data loading external interfaces are neither available nor used for other TOE operations.
- TSF data may be loaded from TOE internal HWRoT and/or other memory

8.7.2 FPT_STM.1 Reliable time stamps

NOTE: Whilst the note at the beginning of this clause states the dependent SFRs are not cited as a distinct requirement an exception applies in this case as reliable time stamps are either explicit or implicit across logging and verification functions of the TOE.

FPT_STM.1.1: The TSF shall be able to provide reliable time stamps.

8.7.3 FPT_HWROT.1 Root of Trust based on hardware

NOTE: The text in this clause is identical to that given in clause 7.1 (with the exception of referencing to table numbers) where it appears as the definition of the SFR family, and in the current clause it appears as the formal SFR instantiation

FPT_HWROT.1.1: The TSF shall contain an immutable root of trust that contains trusted data [**selection, choose one of: certificate, public key, hash of public key/s, hash of certificates, [assignment: other credential values]**], which are preserved in ***[selection:***

a. a One-Time-Programmable (OTP) memory;

b. a dedicated security component;

c. [assignment: other HW components]

].

8.8 TOE access class

8.8.1 FTA_SSL.3 TSF-initiated termination

As a standalone autonomous device the TOE/OND is assumed to be available without interruption in its normal operational mode. Where an operation such as local or remote management invokes a dedicated interactive session that session shall terminate that session after a configurable time interval, where the timer is started on completion of any interaction and be reset if any interaction is detected.

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

8.9 Trusted Path class

8.9.1 Overview of provisions

As declared in ETSI TS 103 962 [1] and ETSI TS 103 963 [2] for each of Requirements 8, 28 and 66 it is required to establish a secured channel for communication of an external user to the TSF. The only external relationship envisaged is between the TSF and its remote management function.

Requirement 8 states that all entities shall be able to report the form of CIA protections that are available and operational to authorized entities. The provisions are therefore to be able to report on the means of giving assurance of the integrity of data transferred, the authenticity of the data transferred, and the confidentiality of the transferred data.

NOTE 1: The communications channels between the TSF for transfer of customer communications are not addressed as those communications are not visible to the TSF.

NOTE 2: Notwithstanding the remote system being operated by a human user there is no user to device relationship in the OND, thus the trusted path as defined in CC-Part 2 [5] is suppressed in favour of the trusted channel defined in CC-Part 2 [5].

NOTE 3: Where a user session to remotely access critical data on the TOE/OND is required the provisions of a privileged access workstation described in ETSI TS 103 994 [i.11] and in ETSI GR NFV-SEC 007 [i.12] may be taken into account.

8.9.2 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 ***the TSF, the remote management entity*** to initiate communication via the trusted channel.

FTP_ITC.1.3: The TSF shall initiate communication via the trusted channel for transfer of management information and control.

9 Security Functional Requirements Rationale

In addition to the rationale for the SFRs that are derived from requirements in ETSI TS 103 962 [1] and ETSI TS 103 963 [2] and mapped in Annex A the detail mapping is given in Table 11.

Table 11: Mapping from objectives to SFRs and the rationale to select each SFR

Objective	SFR	Rational
O.CONF_01: The content of a transmission should not be available to an attacker even if the raw data is intercepted.	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 and files 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	The related cryptographic operations protect the data transmitted from disclosure.
	FCS_RNG.1	Quality key material generation requires quality random numbers as input which this SFR provides.
		The objective is covered.
O.AVAIL_01: Endpoints of each link should be uniquely identifiable, and should be able to verify their identity.	FIA_API.1	The SFR ensures that each entity is identified with properties it has to have. That ensures unique identification.
	FIA_ATD.1	Unique user attributes are defined and serve for identification and authentication procedures.
		The objective is covered.
O.AVAIL_02: Data (content, control, signalling) that is essential to the management of the network should only be visible to authorized entities in the network.	FDP_ACC.1	Access to data requires passing the authentication policy this SFR provides. Only successfully authenticated users can access the data.
	FDP_ACF.1	Access to data is only granted when the access control policy was passed which requires the presence of the security attributes meeting the policy rules.
	FIA_ATD.1	The SFR defines the attributes that are essential for passing the access controls.
	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 authorization of the user before identification. That ensures that unallowed access to data and resources is not practical.
	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 authorized 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 authorized users can access these data.
	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 prerequisite for the access control policy.
	FMT_SMF.1	This SFR enables the specification of the user accounts, roles and the assignment of the rights respectively privileges. It ensures that users have the right role with the right authorization based on rights and privileges.
	FPT_INI.1	This SFR ensures the secure TSF initialization including that the authentication and authorization procedures are in place when the TOE achieves normal operational status after a startup or reset.
		The objective is covered.
O.DataFilter: The TOE shall ensure that only allowed management traffic goes through the TOE.	FDP_ACC.1	Access to management data requires passing the authentication policy this SFR provides. Only successfully authenticated users can access the data. Authenticated users will not induce malicious data traffic.
	FDP_ACF.1	Access to data is only granted when the access control policy was passed which requires the presence of the security attributes meeting the policy rules. Authenticated users will not induce malicious data traffic.
	FMT_SMF.1	The SFR include the specification of operation management which includes functions that control the traffic on the management channel.
	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 authorized modifications of security parameters are operated.

Objective	SFR	Rational
	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 authorized users can access these data.
		The objective is covered.
O.Authentication: The TOE shall authenticate users before access to data and security functions is granted. Refer to clause 5.2 of ETSI TS 103 924 [12].	FCS_COP.1	Cryptographic operations include the verification of presented credentials for their validity.
	FIA_AFL.1	This SFR ensures that failed authentications are treated properly and protect from bypassing authentication controls.
	FIA_ATD.1	The SFR defines the attributes that are essential for passing the access controls.
	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 authorization of the user before identification. That ensures that unallowed access to data and resources is not practical.
	FDP_ACC.1	Access to the TOE 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.
	FPT_INI.1	This SFR ensures the secure TSF initialization including that the authentication and authorization procedures are in place when the TOE achieves normal operational status after a startup or reset.
	FPT_HWROT.1	The credentials therein are immutable by hardware protection and ensure that only authenticated and integrity correct is executed that from the TSF right after a startup or reset.
	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.
	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.
	FDP_SDC.1	This SFR ensures that stored data are confidentiality protected which holds specifically for threat agent that managed bypassing the access controls and access memories. Those threat agents might see only encrypted data.
		The objective is covered.
O.Authorization: The TOE shall implement different authorization roles that can be assigned to users in order to restrict the functionality that is available to them.	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 authorization.
	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 authorized 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 authorized users can access these data.
	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 prerequisite for the access control policy.
	FMT_SMF.1	The SFR finally assigns the attributes to the user role and authorizes thereby the user in its roles and manages the rights.
	FDP_SDC.1	This SFR ensures that stored data are confidentiality protected which holds specifically for unauthorized users accessing memories. Those might see only encrypted data.
		The objective is covered.
O.Audit: The TOE shall provide functionality generate audit records for security-relevant administrator actions.	FAU_GEN.1	This SFR ensures the logging of security relevant events including defined user (administrator) activities.
	FPT_STM.1	For analysis purpose the exact time or time sequences of events is crucial and this SFR ensures that logging records come with reliable time stamps.
		The objective is covered.

Objective	SFR	Rational
O.Communication: The TOE shall implement logical protection means to ensure integrity and confidentiality for the network communication between the TOE and Network Management System(NMS) as well as the TOE and trusted IT products from the operational environment. This objective refers to the requirements stated in clauses 6.1 and 7.2 of ETSI TS 103 924 [12].	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	The related cryptographic operations protect the data transmitted from disclosure.
	FCS_RNG.1	Quality key material generation requires quality random numbers as input which this SFR provides.
	FIA_AFL.1	This SFR ensures that failed authentications between communication entities are treated properly and protect from bypassing authentication controls.
	FIA_ATD.1	The SFR defines the attributes that are essential for passing the access controls. As only identified and authenticated entities are enabled to set up a communication channel with the TOE.
	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 only identified and authenticated entities are enabled to set up a communication channel with the TOE.
	FIA_UID.1	This SFR ensures that the TOE first executes on user initiation only actions that serve for authorization of the user before identification. That ensures that only identified and authenticated entities are enabled to set up a communication channel with the TOE.
	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.
		The objective is covered.
O.SecurityManagement: The TOE shall provide functionality to manage security functions provided by the TOE. Refer to ETSI TS 103 924 [12], clause 4.4.	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 authorized 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 authorized users can access these data.
	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 prerequisite for the access control policy protecting the security functions.
	FMT_SMF.1	The SFR finally assigns the attributes to the user role and authorizes thereby the user in its roles and manages the rights including those for the security functions.
		The objective is covered.
O.SWVerification: The TOE shall provide functionality to allow code loading only when it was prior successfully verified in terms of authenticity, integrity and version. This objective includes updates and patches from external.	FDP_SDI.1	This SFR ensures that code retrieved from TOE is integrity verified before the code gets executed.
	FPT_INI.1	This SFR ensures the secure TSF initialization including the verification of authenticity, integrity and version control.
	FPT_HWROT.1	The credentials therein are immutable by hardware protection and provided to the means that ensure that only authenticated and integrity correct code is loaded for execution.
		The objective is covered.

10 Security Assurance Requirements

10.1 Rationale for the Security Assurance Requirements

The CC process, in very simple terms, asks an evaluator to verify the efficacy of the implementation of security requirements. The security requirements for the ONDS domain are specified in ETSI TS 103 962 [1] and ETSI TS 103 963 [2] derived from the common catalogue in ETSI TS 103 924 [12] and have been identified as essential requirements by the conduct of a targeted TVRA exercise (see ETSI TS 102 165-1 [i.1] for details of the method applied, and Annex A of ETSI TS 103 924 [12] for the documentation of the conducted exercise). The assignment of a verdict by an evaluator against the functional requirements, given in the CC SFR format in clause 8 (derived from the baseline requirements in ETSI TS 103 962 [1] and ETSI TS 103 963 [2]), is guided by the identification of specific Security Assurance Requirements (SARs) defined in the present clause. The SARs are given in the form identified in CC from the set of security assurance components as defined in CC-Part 3 [6]. The selection of such components is intended to ensure that the overall assurance claim given in clause 5 of the present document is met.

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 CC-Part 3 [6] and claimed in clause 4 with the targeted evaluation assurance level. Table 12 summarizes the dependencies of each of the identified SARs from the main body of the present document and the resolution of them in the present document.

NOTE: The assurance level identified in clause 4.2.6 is "EAL3 augmented with ALC_FLR.2" as this is consistent with the substantial assurance level identified in the CSA [i.26] and to which the present document is designed to be conformant to.

Table 12: Security Assurance Requirements Dependency

Security Assurance Requirement	Dependency from CC-Part 3 [6]	Resolution
ADV_ARC.1: Security architecture description	ADV_FSP.1: Basic functional specification ADV_TDS.1: Basic design	ADV_FSP.1 ADV_TDS.1
ADV_FSP.1: Basic functional specification	No dependencies	N/A
ADV_FSP.3: Functional specification with complete summary	ADV_TDS.1	ADV_TDS.1
ADV_TDS.1	ADV_FSP.2: Security-enforcing functional specification ADV_FSP.3: Functional specification with complete summary	ADV_FSP.3
ADV_TDS.2: Architectural design	ADV_FSP.3: Functional specification with complete summary	ADV_FSP.3
AGD_OPE.1: Operational user guidance	ADV_FSP.1: Basic functional specification	ADV_FSP.1
ALC_CMC.3: Configuration management capabilities - authorized controls	ALC_CMS.1: TOE CM coverage ALC_DVS.1: Identification of security measures ALC_LCD.1: Developer defined life-cycle processes	ALC_CMS.3
ALC_CMS.3: Configuration management scope - Implementation representation CM coverage	No dependencies	N/A
ALC_FLR.2: Flaw reporting procedures	No dependencies	N/A
AVA_VAN.2: Vulnerability survey	ADV_ARC.1: Security architecture description ADV_FSP.2: Security-enforcing functional specification ADV_TDS.1: Basic design AGD_OPE.1: Operational user guidance AGD_PRE.1: Preparative procedures	ADV_ARC.1 ADV_FSP.3 ADV_TDS.1 AGD_OPE.1
NOTE 1: For ALC_DVS.1, the intent is met by the present document and the core references. NOTE 2: For ALC_LCD.1, the application is outside of the scope of the present document. NOTE 3: For AGD_PRE.1, the application is outside of the scope of the present document.		

Annex A (normative): Definitions for SAR software patch management

A.1 Software patch management overview

NOTE: The present annex only addresses software patch management where such an update or patch is intended to address vulnerabilities in the software, where vulnerabilities are introduced by misconfiguration or user error the provisions here do not apply.

The requirements given in clause C.1, Table C.4 of ETSI TS 103 962 [1] and ETSI TS 103 963 [2] apply to the general provisions for identification, reporting and mitigating vulnerabilities in the TOE's software (see also clause 7.2.1 of the present document).

A.2 Software Function Policy extensions

The following Security Function Policy (SFP) enables the management of the secure availability of the SW patch. The patch shall be managed by the TOE's management entity and shall only be installed if the access control policy conditions are met (i.e. the access control policy shall include rules to evaluate the authority of the installer to install any update).

The TOE shall assure the integrity and authenticity of the received software update. The public key used to verify the software update may be provisioned and updated independently of the provision of the update.

NOTE 1: The means by which the software update is made available is not addressed in the present document.

NOTE 2: The signature and identifier of the current software version is expected to be maintained in a persistent storage area in order to allow for the validity of the update to be verified.

It is recognized that software updates that address vulnerabilities reported as part of a vulnerability reporting scheme should be made available through the reporting scheme (see the NIS2 Directive [i.17]).

The following subject and object with attributes related to SW Update SFP are added.

Table A.2.1: Subject and object attributes related to SW Update SFP

Subject/Object/ Information	Description	Security attributes
S.O-UPD	On-TOE patch mechanism: component in charge of Software Update handling, it is a part of the TSF.	Current version: Attribute of the last successfully installed software update, specifying its version. TSF data, which is stored persistently in the TOE.
S.UPDTER	It is assumed that an authorized administrator operates remotely at the management centre. The management centre retrieves the version information from the TOE and conducts the TOE update only where the access control conditions are satisfied (i.e. the update is valid and newer than the installed software). These operations change the TOE and require authorization of the device against the TOE. (see note 1)	Authentication credentials of a local or remote administrator. Authorization of the update device.

Subject/Object/ Information	Description	Security attributes
Obj.PatchUpdate	The patch image loaded into the TOE to replace/update in whole or in part the current update-able TOE software. The patch forms part of the TOE. If the software update process is successful the updated software is the new operational software. For the software update process to be considered successful all steps, including any necessary decryption, the verification and validation steps, and final testing after activation shall complete without error. (see note 2)	New version: Attribute of the patch image specifying its version. Presented to the TOE during the software update process and stored as current software version in the TOE, if the update was successful. Signature and proof of authenticity: attribute of the patch image and its version, in terms of a signature over both. Verification by the TOE during the software update process. The generation can only be at the management centre, as only the management centre can access and use the signing private key.
Obj.AUDR	Audit records reporting success or failure of the security activities of the on-TOE-patch-mechanisms signature verification, installation, and activation.	The patch update process can record only one of the following values: Installed without error; or Discarded (i.e. installation or verification failed). The log record may store additional data in the case of Discarded to clarify the reason the update has been discarded. The log record shall by default indicate the identity of the update, and the time and location (e.g. device identity and system address) of the update. (see note 3)
NOTE 1: Where the updater is local to the device it is not considered further in the present document. NOTE 2: Once a software element has been updated only the log record should be able to show that a patch or update has been applied as the software element is considered complete when operational. NOTE 3: The developer shall independently verify the efficacy of the update process and the update of each individual patch prior to its distribution to a live system (this is consistent with the requirements stated in clause 5.3 of ETSI TS 103 645 [i.15]).		

The following SW Update SFP operations are added.

Table A.2.2: Added SW Update SFP operation

Operation	Definition
OP.SWU	Software update
OP.REA	Read out Obj.AUDR

The TOE enforces this SFP to securely manage the object Obj.PatchUpdate during OP.SWU operation.

The following access control SFR extensions are added.

Table A.2.3: Access Control SFR extensions

Item	Definition
S.O-UPD	The component that manages the SW update
Obj.PatchUpdate	The signed patch image
OP.SWU	The operation that updates the current with the updated SW

A.3 Software Functional Requirement provisions for software update

A.3.1 Access control

The core provisions for access control defined in clause 8.4 of the present document apply with the following extensions.

The following rules shall be added to FDP_ACF.1:

- The TSF shall enforce the SW Update SFP to objects based on the following:
  - Subjects: S.O-UPD;
  - Objects: Obj.PatchUpdate;
  - Security Attributes or conditions:
    - Update version is valid, software update image signature has been verified as true, Current version is older than the proposed update.
- The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
  - S.O-UPD is allowed to perform OP.SWU, i.e. to import Obj.PatchUpdate according to FDP_ITC.2/UPD, if:
    - the Software Update Signature over Obj.PatchUpdate and New version are successfully verified; and
    - new version constitutes an update for the current version.

A.3.2 Rollback functionality

In the case that an update fails, for any reason, it is necessary to allow the system to be recovered to a prior state, this is addressed by the rollback functionality and the functional requirements listed in Table A.3.1 below.

Table A.3.1: FDP_ROl.1/UPD Basic rollback

FDP_ROL.1/UPD Basic rollback	
FDP_ROL.1.1/UPD	The TSF shall enforce the **SW Update SFP** to permit the rollback of the **unsuccessful or interrupted OP.SWU** on the **Obj.PatchUpdate**.
FDP_ROL.1.2/UPD	The TSF shall permit operations to be rolled back **when the OP.SWU failed**.
FPT_RCV.4/UPD Function recovery	
FPT_RCV.4.1/UPD	The TSF shall ensure that [**interruption or incident which prevents the successful execution and completion of the update operation (OP.SWU)**] have the property that the function either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

A.4 Rationale tables for extensions arising from Software Update functionality

Table A.4.1: Security Requirements Dependency Rationale for Software update functionality

SFR	Dependency (from clause A.3)	Resolution
FDP_ROL.1/UPD Basic Rollback	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information access control	FDP_ACC.1
FPT_RCV.4/UPD Function recovery	No dependencies	N/A

Table A.4.2: Security Functional Requirements Rationale

Objective (from clause 6.6)	SFR (from clause A.3)	Rationale
O.SWVerification	FDP_ROL.1/UPD Basic Rollback	This requirement ensures that the TOE has the capability to rollback to the unchanged software in the case of an update failure, update interruption, or when the software update failed for any other reason.
	FPT_RCV.4/UPD Function recovery	This requirement ensures that the TOE can be recovered from any failure state caused by a software update failure to the state it was in before the update was attempted.
		The objective is covered.

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

Table B.1 identifies the base requirements from ETSI TS 103 962 [1] and ETSI TS 103 963 [2] and provides a simplified analysis of each requirement to identify a mapping to applicable SFRs from CC-Part 2 [5] (see also the expanded SFR modelling given in clause 8 of the present document). The statements in column 2 are quoted from ETSI TS 103 962 [1] and ETSI TS 103 963 [2] and are not normative in the context of the present document.

NOTE 1: The mapping offered is not the only possible mapping and a developer may be able to identify others, thus the present mapping is indicative but shows the preferred mapping from ETSI TS 103 962 [1] and ETSI TS 103 963 [2] to the present document.

NOTE 2: The mapping given in the present document is marked as informative and is not in the scope of evaluation of the PP.

Table B.1

Item	Requirement	Status	Requirement analysis for test and evaluation	Applicable PP SFR (from CC-Part 2 [5])
Req-1	An access device shall distinguish and keep separate the user and network domains in the device.	M	This cannot be addressed in an automated test, rather this can only be evaluated based on the evaluation of design records of the manufactured devices (and the resulting TOE).	NA
Req-2	ON systems shall be designed to be secure by default and to support the functionality required by the CIA paradigm.	M	This cannot be addressed in an automated test, rather this can only be evaluated based on the evaluation of design records of the manufactured devices (and the resulting TOE).	NA
Req-3	At initialization and at runtime all links shall be established and security associations created within the trust and security policy established by the operator of the equipment/network.	M	This requires a mapping between the policy set externally to the TOE and its enforcement in the device.	FIA_UID.1: Timing of identification FIA_UAU.1: Timing of authentication
Req-4	Any link enabled during, and post-initialization, shall support periodic re-establishment of the security association.	M	This is closely linked to Requirements 2, 3, 5 and 6. The system can re-establish a security association by use of a timer or some other event. In essence the current security association is terminated and a new one re-established.	FTA_SSL.3: TSF-initiated termination
Req-5	The principles of least privilege and least persistence shall apply to all security associations.	M	The base documents extend this by requiring Policy and Attribute Based Access Control. The policy enforces the level of privilege and the time limit of the access, therefore the test environment should be able to determine if the policy is violated either by privilege escalation or by extension of the time an association is allowed to remain live.	NA
Req-6	In accordance with the least persistence principle security associations shall not be maintained for longer than required.	M	The specific time that is established for a security association to be allowed to be maintained is defined in the configuration data.	FTA_SSL.3: TSF-initiated termination

Item	Requirement	Status	Requirement analysis for test and evaluation	Applicable PP SFR (from CC-Part 2 [5])
Req-7	If any software verification fails that software and any supporting elements shall not participate in any security association.	M	It is assumed that software is a digitally signed object and that all software has its signature verified before instantiation. If the signature fails this shall be identified.	FCS_COP.1 FMT_SMF.1: Specification of Management Functions FPT_INI.1: TSF initialization
Req-8	All ON entities shall be able to report the form of CIA protections that are available and operational to authorized entities.	M	This is nominally part of the audit of material on the TOE and the access to the information is part of the access control policy. It is clear that in establishing a secure channel the negotiation protocol is able to verify that both sides of the channel support the same CIA operations with the same parameterization.	FTP_ICT.1: Inter-TSF trusted channel
Req-9	An OAN device shall be integrated to the wider ON and telecommunications system of which it is a component.	M	This cannot be addressed in an automated test, rather this can only be evaluated based on the evaluation of design records of the manufactured devices (and the resulting TOE).	NA
Req-10	An OAN device shall consist of at least 1 (one) execution environment.	M	This cannot be addressed in an automated test, rather this can only be evaluated based on the evaluation of design records of the manufactured devices (and the resulting TOE).	NA
Req-11	An OAN device's execution environment shall have 1 (one) initial root of trust.	M	This cannot be addressed in an automated test, rather this can only be evaluated based on the evaluation of design records of the manufactured devices (and the resulting TOE).	FPT_HWROT.1: Root of trust based on HW
Req-12	The execution environment shall have at least one executable code block.	M	This cannot be addressed in an automated test, rather this can only be evaluated based on the evaluation of design records of the manufactured devices (and the resulting TOE).	NA
Req-13	There should be a discrete execution environment for each side and discrete roots of trust for each side.	R	This cannot be addressed in an automated test, rather this can only be evaluated based on the evaluation of design records of the manufactured devices (and the resulting TOE).	NA
Req-14	If an OAN device supports a multi-occupancy client environment it shall provide confidentiality services at the client side to ensure physical and cryptographic separation of distinct clients.	M C	Notionally the encryption of data links to the client is out of scope of the TOE as the service provision is external to the TOE (the optical links are out of scope).	NA
Req-15	The OAN Device shall have a root of trust used for initialization to enable secure boot capabilities.	M	This cannot be addressed in an automated test, rather this can only be evaluated based on the evaluation of design records of the manufactured devices (and the resulting TOE).	FPT_HWROT.1: Root of trust based on HW FPT_INI.1
Req-16	The OAN Device shall implement a root of trust where the scope of functions enabled by the root of trust shall be defined in succeeding clauses of the present document.	M	This cannot be addressed in an automated test, rather this can only be evaluated based on the evaluation of design records of the manufactured devices (and the resulting TOE).	FPT_HWROT.1: Root of trust based on HW FPT_INI.1: TSF initialization
Req-17	The guidelines given in NIST SP 800-164 [i.20] shall be followed in order to provide the following local (device specific) trust services: Root of Trust for Storage (RTS); Root of Trust for Verification (RTV); Policy Enforcement Engine.	M	This cannot be addressed in an automated test, rather this can only be evaluated based on the evaluation of design records of the manufactured devices (and the resulting TOE).	FPT_HWROT.1: Root of trust based on HW
Req-18	The manufacturer of the OAN Device shall attest to the provision of the root of trust by reference to the method applied.	M	This cannot be addressed in an automated test, rather this can only be evaluated based on the evaluation of design records of the manufactured devices (and the resulting TOE).	NA

Item	Requirement	Status	Requirement analysis for test and evaluation	Applicable PP SFR (from CC-Part 2 [5])
Req-19	The manufacturer of the OAN Device shall publish the attestation of the provision of the root of trust in the technical specification of the OAN Device.	M	This cannot be addressed in an automated test, rather this can only be evaluated based on the evaluation of design records of the manufactured devices (and the resulting TOE).	NA
Req-20	The presence of the hardware root of trust shall be asserted by a platform specific attribute certificate.	M	This cannot be addressed in an automated test, rather this can only be evaluated based on the evaluation of design records of the manufactured devices (and the resulting TOE).	NA
Req-21	All cryptographic modules shall be designed to be crypto-agile.	M	This cannot be addressed in an automated test, rather this can only be evaluated based on the evaluation of design records of the manufactured devices (and the resulting TOE).	NA
Req-22	The specific cryptographic algorithms for each security association shall be defined by the security policy.	M	This requires visibility of the security policy, set by the external management entity.	NA
Req-23	Cryptographic algorithms should be sufficient to inhibit known cryptanalysis attacks and mechanisms.	R	This requires the adoption of best practice cryptography.	FCS_COP.1.1
Req-24	The broad assumption that the key is secure applies and therefore **advice on exploits of key material should be made available** and key update mechanisms implemented to inhibit attacks using such exploited key material.	R	This cannot be addressed in an automated test, rather this can only be evaluated based on the evaluation of design records of the manufactured devices (and the resulting TOE).	FMT_SMF.1 FCS_CKM.2 FCS_CKM.6
Req-25	The security processes shall be self-monitoring and report detected errors to the local security authority which may in turn report errors to a remote, central, security authority.	M	This is part of the overall system audit and management.	NA
Req-26	All ON devices shall be identified with a canonical/root identity and, optionally, additional semantic identifiers identifying their functional nature.	M	The forms of identifier.	FIA_UID.1
Req-27	Where provided, the semantic identifier shall be used to indicate the functional nature of the entity.	M C	This is part of the overall identity management framework of the entire network and allows for the management entity to map functionality across the devices of the network. It is likely to be validated only by examination of the identity management framework which is outside the scope of the TOE described in the present document.	NA
Req-28	The attestation of function shall be verifiable by reference to a 3rd party.	M	The attribute, consistent with the model from ETSI TS 103 486 [i.24], assumes for each attestable attribute there is an attribute authority that assigns and verifies it.	FIA_ATD.1 FTP_ITC.1
Req-29	The authentication process shall verify the ON entity's identity (e.g. a globally unique device address) to a shared key assignment.	M	The shared key assignment can be either a symmetric (shared) key, or by means of asymmetric keying where the public key element is shared.	FIA_API
Req-30	The to be authenticated identity shall be an attribute of the authentication protocol.	M	This is part of the identification and authentication protocol. When using asymmetric encryption where the public key is shared in a certificate the certificate contains the identity. It has to be clear what exactly is being authenticated by the protocol. It is also stated in ETSI TS 103 962 [1] and ETSI TS 103 963 [2] that only cryptographically relevant forms of authentication are considered.	FCS_COP.1 FTP_ITC.1

Item	Requirement	Status	Requirement analysis for test and evaluation	Applicable PP SFR (from CC-Part 2 [5])
Req-31	The identity shall always be authenticated on first presentation and periodically thereafter.	M	See Requirement 6.	FIA_API
Req-32	In order to be consistent with the principle of least persistence an authenticated session shall expire after a set time.	M	See Requirement 6.	FTA_SSL.3: TSF-initiated termination
Req-33	The length of an authentication session shall be set by the Authentication-Session-Time-Limit variable.	M	See Requirement 6.	FTA_SSL.3: TSF-initiated termination
Req-34	The Authentication-Session-Time-Limit variable shall be established for each security association.	M	See Requirement 6.	FTA_SSL.3: TSF-initiated termination
Req-35	A device shall be identified in order to be admitted to the operator's trust domain.	M	The trust domain is established in the network management centre.	FIA_UID.2
Req-36	Within the trust domain the trust domain manager shall verify the capability of each device.	M	The trust domain manager authenticates the capability of the device.	FIA_UAU FIA_ATD.1
Req-37	An ON device shall present an identifier to each of the client and the network side of the device.	M		FIA_UID.1 FIA_API.1
Req-38	It should not be feasible to determine/infer the identifier presented to one side from knowledge of the identifier presented to the other side.	R	This requires strict separation of the two faces of the device.	FTP_ITC.1
Req-39	Any identifier presented by the device shall be authenticated by the receiving device.	M		NA
Req-40	A key shall be associated to an attribute or identifier of the OAN Device.	M		FTP_ITC.1
Req-41	The binding of key to the attribute or identifier shall be maintained for each security association.	M		FMT_SMF.1 FCS_CKM.2 FCS_CKM.3 FCS_CKM.6
Req-42	A symmetric keyed security association shall identify the following elements: Associated identity or Associated capability; Root key-id (if part of a key hierarchy); CIA purpose (one of authentication, encryption, integrity); Algorithm.	M		NA
Req-43	A Message Authentication Code (MAC) method should be used in established security associations as an alternative to simple integrity check functions where the integrity, MAC, key is pre-defined or established as a session specific key.	R		FTP_ITC.1
Req-44	The MAC approach to authentication as outlined in ETSI TS 102 165-2 [14] shall apply.	M		FTP_ITC.1
Req-45	challenges used in any MAC based authentication shall be generated using a true source of randomness.	M	This is a simple requirement placed on any random number.	FCS_RNG.1
Req-46	Software only functions shall not be used to generate random challenges.	M	This is a simple requirement placed on any random number.	FCS_RNG.1

Item	Requirement	Status	Requirement analysis for test and evaluation	Applicable PP SFR (from CC-Part 2 [5])
Req-47	A challenge-response method should be used at initialization and for key establishment, key refresh, events.	R	This applies to the timing of authentication.	FIA_UAU.1
Req-48	Only cryptographically relevant challenge response schemes shall be used.	M	This refers to the form of the authentication.	FCS_COP.1
Req-49	The challenge response approach to authentication as outlined in ETSI TS 102 165-2 [14] shall apply.	M	This is just one of many approaches to authentication and applies only where Req-48 is satisfied which in turn requires Req-47 to be implemented.	FMT_SMF.1 FTP_ITC.1
Req-50	Random challenges used in any challenge-response protocol shall be generated using a true source of randomness.	M	This is a simple requirement placed on any random number.	FCS_RNG.1
Req-51	A device should only be able to perform a self-attestation of its identity at initialization.	R	This applies to the timing of authentication.	FIA_UAU.1
Req-52	The self-attestation shall be provided in the form of a digital signature and include a signed public key.	M C	This requires digital signature and distribution of the public key.	FCS_COP.1 FCS_CKM.2
Req-53	In order to perform self-attestation of identity the OAN device shall be able to securely generate cryptographic keys associated with identifiers, and to securely store the private cryptographic material.	M C	This requires the generation of a cryptographic key pair with characteristics matched to the signature algorithm.	FCS_CKM.1.1
Req-54	The OAN device shall have a source of true randomness with entropy at least equal to the required security strength of the cryptographic operations that rely upon this randomness.	M	This is a simple requirement placed on any random number.	FCS_RNG.1
Req-55	The OAN device shall have a root of trust for storage to store private cryptographic material (private key).	M	Whilst the requirement identifies a root of trust (e.g. a TPM) the implied requirement is that the store provides assurance of confidentiality and integrity of the stored data. In addition, there is an underlying requirement that access to the stored data i(i.e. the private key) is only available to appropriate cryptographic operations.	FDP_SDC.1 FDP_SDI.1 FPT_HWROT.1: Root of trust based on HW
Req-56	In accordance with ETSI TS 103 486 [i.24] the identity (canonical) and identifying attributes of a device should be attested to by an appropriate independent 3rd party.	R	The assumption underpinning this is that attestations are made using a cryptographically relevant attribute attestation (e.g. an X.509 attribute certificate biding the attribute, identity and key pair).	FCS_COP.1
Req-57	Proofs of identity shall be made available to corresponding parties using identity based public key certificates that clearly identify the attesting authority and that are able to resolve to the Root Authority for the trust domain.	M	This is a requirement of the format of the public key certificate and the architecture of the public key infrastructure.	FTM_SMF.1
Req-58	A device should only be able to perform a self-attestation of its capability at initialization.	R C	This applies to the timing of authentication.	FIA_UAU.1
Req-59	The self-attestation shall be provided in the form of a digital signature and include a self-signed public key.	M C	The assumption underpinning this is that attestations are made using a cryptographically relevant attribute attestation (e.g. an X.509 attribute certificate biding the attribute, identity and key pair).	FCS_COP.1

Item	Requirement	Status	Requirement analysis for test and evaluation	Applicable PP SFR (from CC-Part 2 [5])
Req-60	Identifying attributes of a device should be attested to by an independent 3rd party. The public key of the relevant attribute authority should be installed locally to the device.	R	There are requirements here for storage and for the attestation by a cryptographic process.	FCS_COP.1 FDP_SDC.1
Req-61	Proofs of identity shall be made available to corresponding parties using an attribute based public key certificate that clearly identify the attesting authority and that are able to resolve to the Root Authority for the trust domain.	R	This refers to the structure of the proof of authentication.	FCS_COP.1
Req-62	All exchanged discrete messages shall have their integrity verified on reception at the device.	M		FTP_ITC.1
Req-63	The integrity check function shall be cryptographically strong and may be included in a MAC for symmetric keyed associations, or in a digital signature for asymmetric keyed associations.	M	The primary concern here is the cryptographic method for applying the integrity check value.	FTP_ITC.1
Req-64	Any message that fails the integrity check shall be discarded and an error reported.	M		FTP_ITC.1
Req-65	In order to mitigate against replay attacks a Time Variant Parameter (TVP) should be included with the plaintext prior to calculation of the Integrity Check Value (ICV).	R		FTP_ITC.1
Req-66	All transmissions made from the OLT towards the network should be protected by a confidentiality security association.	R		FTM_SMF.1 FTP_ITC.1
Req-67	Where used the security association should identify: The encryption algorithm; The mode used for application of the algorithm; the end points.	R C		FTM_SMF.1 FTP_ITC.1
Req-68	Where the chosen encryption mode requires a per-block variant parameter (e.g. in counter mode) the means to establish the initial value and increment the variant parameter shall be stated in the security association.	M C	This is related to the cryptographic operation and the parameters used to enable the particular mode of encryption.	FCS_COP.1 FTP_ITC.1
Req-69	Every access device shall have a Root of trust for Storage (RtS).	M	This cannot be addressed in an automated test, rather this can only be evaluated based on the evaluation of design records of the manufactured devices (and the resulting TOE).	FPT_HWROT.1: Root of trust based on HW
Req-70	For an access device there should be independent RtSs for the user/client side and for the network side of the device.	R	This cannot be addressed in an automated test, rather this can only be evaluated based on the evaluation of design records of the manufactured devices (and the resulting TOE).	NA
Req-71	All data in OAN devices shall be made available to authorized entities using the principle of least privilege.	M		FDP_ACC
Req-72	The access control mechanism shall follow the policy model outlined in ETSI TS 102 165-2 [14].	M		FDP_ACC

Item	Requirement	Status	Requirement analysis for test and evaluation	Applicable PP SFR (from CC-Part 2 [5])
Req-73	Each protected Object in the OAN device shall be protected by an access control policy.	M		FDP_ACC FIA_ATD.1: User attribute definition, FDP_ACF.1: Security attribute based access control FMT_MSA.1: Management of security attributes FMT_MSA.3: Static attribute initialization
Req-74	The access control policy shall be evaluated on each access attempt.	M		FDP_ACC FIA_UAU
Req-75	The policy shall consist of 1 or more rules each of which shall be evaluated in turn.	M		FDP_ACF.1
Req-76	Every denied access attempt shall be recorded.	M		FIA_AFL.1
Req-77	The record of each denied access attempt shall include at least the following: subject-identifier; object-identifier; date/time of failed access attempt; logical and (if available) physical location of the object; if available the logical and physical location of the subject.	M		FAU_GEN.1.2
Req-78	If an object has multiple access control errors the OAN device, in collaboration with the ONDS-M, shall set a reporting threshold for making an exception report.	M		FIA_AFL.1
Req-79	If any rule fails because it cannot be determined (the calculation cannot be made for any reason) permission shall not be granted and an exception raised.	M		FDP_ACF.1
Req-80	If an exception is raised it shall include the details of the rule that failed.	M		FIA_AFL.1
Req-81	The default access control condition for all objects shall be "do not allow"/"do not permit".	M		FDP_ACF.1
Req-82	The following rules shall be implemented in OAN devices: CFG-AC; CK-AC; DEV-AC; PAC-AC.	M		NA
Req-83	The overall access control policy should be defined in such a way that all rules of a policy have to pass in order to permit access.	R		FDP_ACF.1
Req-84	A policy shall only set access control permission to True where all rules of any policy pass.	M		FDP_ACF.1

Annex C (informative): Mapping to CRA considerations

NOTE 1: All references in Tables C.1 and C.2 that follow are to the Cyber Resilience Act (CRA) [i.25].

NOTE 2: The mapping given in the present document is marked as informative and is not in the scope of evaluation of the PP.

NOTE 3: The term TOE Resource(s) is used in the mappings below to refer to the TOE and any element of the TOE when decomposed.

Table C.1: Indicative Mapping to CRA considerations

	Essential Requirements as defined in CRA [i.25]	**CC SFR (Substantial)**	**CC SAR (Substantial)**	**Rationale**
Part 1 of CRA [i.25]	Cybersecurity requirements relating to the properties of products with digital elements	None (as a general principle no specific obligations are cited)	None (as a general principle no specific obligations are cited)	This sets out the core principle of the CRA [i.25] and is consistent with the general approach captured in Figure 1 of ETSI TS 102 165-1 [i.1] (note that it may be useful for ETSI TS 102 165-1 [i.1] to show a mapping to the top level assurance families ASE_SPD (Security problem definition), ASE_OBJ (Security objectives) and ASE_REQ (Security requirements) from CC-Part 3 [6]).
	(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 – authorized controls ALC_CMS.3: Configuration management scope – Implementation representation CM coverage ADV_TDS.1 or ADV_TDS.2: TDS design	As above this is a core principle of the CRA. A number of approaches to risk assessment exist and a number of controls exist to manage risk. The approaches in ETSI TS 102 165-1 [i.1] supplemented by considerations of vulnerability assessment and penetration testing given in ETSI TS 102 165-2 [14], and the application of security controls in ETSI TR 103 305-1 [i.14] all apply to achieve the overall aim of the CRA. 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 authorized, reviewed, managed, controlled, tested and formally accepted components can be made an implemented part of the TOE. This is closely related to bills of material for hardware and software components in the system.

				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 authorized access controls to the configuration list, parts, and implementation representation. Thereby, it assures that modifications were done in "controlled manner with proper authorizations" 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.
	(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	Noting that ETSI TR 103 305 [i.14] has security controls for the management and inventory of the system assets, and that ETSI TS 102 165-1 [i.1] requires clear identification of all assets, then further mapping of the exercises undertaken to conform to these documents are further evidenced in the application of assurance class APE_SPD which requires identification of the assets, threats and 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.
	(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 (to specify device has reset ability) 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	FMT_SMF.1: Management of security functions(to specify device has update ability)	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 specify the management functions or mechanisms for the conduct of the TOE security update.

		opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;			It should be noted that vulnerabilities introduced by inappropriate configuration are not addressed here but that reasonable application of good user interfaces to the configuration settings and capture of inappropriate configuration combinations. 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 CC-Part 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.
	(d)	ensure protection from unauthorized access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorized access;	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 authentication, the TOE assigns security attributes to the (*now 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 by the authenticated entity. FDP_ACF.1: This SFR implements the access control functions assigned by the security attributes and is linked with FDP_ACC.1 (i.e. these SFRs are co-dependent). 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_SDC.1: Stored data confidentiality (at rest) FTP_ITC.1: Inter-TSF trusted channel (transmit)		FDP_SDC.1: This SFR provides the confidentiality protection of stored data in defined types and in defined memory types. 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 authorized by the user, and report on corruptions;	FDP_SDI.1: Stored data integrity monitoring (at rest) FTP_ITC.1: Inter-TSF trusted channel (transmit)		FDP_SDI.1: This SFR provides the integrity protection of stored data in containers depending on user data attributes. 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 (for ONDS as there is no personal data).
	(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. 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.
	(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 FPT_RCV.4/UPD: Trusted Recovery - FMT_SMR.1: Security roles FDP_SDC.1: Stored data confidentiality (at rest)	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 authorized for accessing the corresponding TOE resources. That means that even if he could bypass the identification and authentication controls he still needs to have authorization to access TOE resources. FPT_RCV.4/UPD: This SFR contributes to the mitigation of an incident as the TOE limits its effects by either completing the update successfully, or otherwise achieves a secure state for enabling manual corrections. FDP_SDC.1: This SFR provides that stored data are encrypted. A threat agent able to bypass authentication is restricted to access only encrypted data. The reason is the missing authorization to access the resource in normal operation. 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 TSF 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.

	(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 no longer needed (thus giving protection 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 C.2

	Essential Requirements as defined in CRA [i.25]	**CC SFR (Substantial-EAL3)**	**CC SAR (Substantial-EAL3)**	**Rationale**
Part 2 of CRA [i.25]	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. 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.	(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

	Essential Requirements as defined in CRA [i.25]	CC SFR (Substantial-EAL3)	CC SAR (Substantial-EAL3)	Rationale
				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. The EUCC surveillance mechanism implicitly fulfil the requirement as regular reassessment and lifetime limitation are present.	(3) is covered by the vulnerability assessment and the certificate maintenance procedures of the EUCC scheme.
	(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.	(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 to the user.
	(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 with the iteration of ALC_FLR.2.
	(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	(7) Covered when: ALC_FLR.2.1D demonstrates secure mechanisms for providing updates, ALC_FLR.2.2D shows

	Essential Requirements as defined in CRA [i.25]	CC SFR (Substantial-EAL3)	CC SAR (Substantial-EAL3)	Rationale
			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.	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 D (informative): Bibliography

- German Federal Office for Information Security, TR 02102 in parts 1 to 3: "Cryptographic Mechanisms: Recommendations and Key Lengths", March 24, 2021.
- German Federal Office for Information Security, BSI: "A proposal for: Functionality classes for random number generators", version 2.0 as of 2011-09-18.
- Annexes to the horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, 2022-09-15.
- ETSI GR QSC 004 (V1.1.1): "Quantum-Safe Cryptography; Quantum-Safe threat assessment".
- ETSI EG 203 310 (V1.1.1): "Quantum Computing Impact on security of ICT Systems; Recommendations on Business Continuity and Algorithm Selection".
- ETSI TS 103 924 (V1.1.1): "Optical Network and Device Security, Catalogue of requirements".
- ETSI TR 103 949 (V1.1.1): "Quantum-Safe Cryptography (QSC) Migration; ITS and C-ITS migration study".
- ETSI GS F5G 014 (V1.1.1): "Fifth Generation Fixed Network (F5G); F5G Network Architecture, Release 2".
- "Collaborative Protection Profile for Network Devices", V2.2.e, 2020-03-23.
- IEC 62443-4-2: "Security for industrial automation and control systems — Part 4-2: Technical security requirements for IACS components".
- draft-ietf-ccamp-gmpls-vcat-lcas-02.txt: "Operating Virtual Concatenation (VCAT) and the Link Capacity Adjustment Scheme (LCAS) with Generalized Multi-Protocol Label Switching (GMPLS)".
- ETSI TS 133 117: "Universal Mobile Telecommunications System (UMTS); LTE; 5G; Catalogue of general security assurance requirements (3GPP TS 33.117 version 17.0.0 Release 17)".
- NIST SP 800-53: "Security and Privacy Controls for Information Systems and Organization", Revision 5, September 2020.
- Recommendation ITU-T Y.1307.2: "Global information infrastructure, internet protocol aspects, next-generation networks, internet protocol aspects – transport, Ethernet virtual private LAN service, Ethernet Virtual Private Line Service".
- Recommendation ITU-T G.8011.3: "Ethernet Virtual Private LAN Service, Transmission systems and digital media, digital systems and networks; series, Packet over transport aspects – Ethernet over transport aspects".
- Recommendation ITU-T Y.1307.3: "Global information infrastructure, internet protocol aspects, next-generation networks, internet protocol aspects – transport, Ethernet virtual private LAN service".
- Recommendation ITU-T Y.1710: "Global information infrastructure, internet protocol aspects – operation administration and maintenance, Requirements for OAM functionality for MPLS networks".
- Recommendation ITU-T Y.1331: "Global information infrastructure, internet protocol aspects, next-generation networks, internet of things and smart cities, Interfaces for the optical transport network".
- ISO/IEC 27001: "Information technology — Security techniques — Information security management systems — Requirements", 2005-10-15.
- Senior Officials Group Systems Security: "Application of Attack Potential to Hardware Devices with Security Boxes", Version 3.0 July 2020.
- Senior Officials Group Systems Security: "SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms", Version 1.2, January 2020.

- Senior Officials Group Systems Security: "Minimum Site Security Requirements", Version 3.0, February 2020.
- ETSI TS 103 732-1: "CYBER; Consumer Mobile Device; Part 1: Base Protection Profile".
- ISO/IEC TS 9569: "Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Patch Management Extension for the ISO/IEC 15408 series and ISO/IEC 18045".

History

Version	Date	Status
V1.1.1	January 2026	Publication