ETSI TS 103 993 V1.1.1 (2025-09)

TECHNICAL SPECIFICATION

Cyber Security (CYBER);
ONDS Test Suite Structure and Test Purposes

Reference
DTS/CYBER-00114

Keywords
cybersecurity, device, optical, TSS&TP

ETSI

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

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

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

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

Modal verbs terminology

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

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

Introduction

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

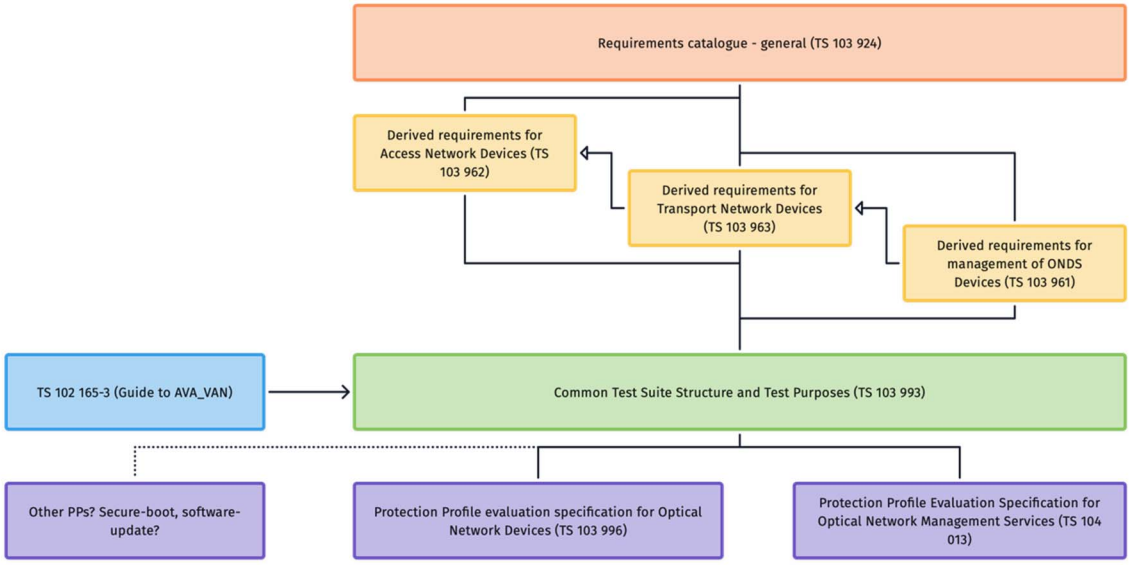

Figure 1: Document structure for Optical Network Device Security

Each of ETSI TS 103 962 [1], ETSI TS 103 963 [2] and ETSI TS 103 961 [5] expand upon the requirements identified in the common catalogue of ETSI TS 103 924 [4]. In the definition of detailed provisions ETSI TS 103 962 [1] acts as the master document with ETSI TS 103 963 [2] and ETSI TS 103 961 [5] 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 (the present document), and from that a specification of the evaluation assessments is derived, to be applied in the form of an EUCC based protection profile (ETSI TS 103 996 [i.4] and ETSI TS 104 013 [i.5]).

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 Test Purposes for ETSI TS 103 962 [1] and ETSI TS 103 963 [2] written in the format of a TSS&TP using the notation TPLan (ETSI ETR 266 [i.8], ETSI ES 202 553 [3]) extended to address the description of test purposes taking into account requirements from Common Criteria Part 2 [8]. The latter is necessary to support conformity to the EUCC programme (for each of CRA [i.1] and NIS2 [i.2] in addition to the CSA [i.3]).

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 ES 202 553: "Methods for Testing and Specification (MTS); TPLan: A notation for expressing Test Purposes".

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

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

[6] 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".

NOTE: This deliverable is being updated and the relevant clause numbering will be retained.

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

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

2.2 Informative references

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

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

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

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

[i.2] Directive (EU) 2022/2555 of the European Parliament and of the 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 (NIS 2 Directive).

[i.3] 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 communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[i.4] ETSI TS 103 996: "Cyber Security (CYBER); ONDS Protection profile - Test cases".

[i.5] ETSI TS 104 013: "Cyber Security (CYBER); ONDS PP for ONDS management protocols and services".

[i.6] ETSI TR 103 866: "Cyber Security (CYBER); Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls".

[i.7] ETSI TS 102 165-3: "Cyber Security (CYBER); Methods and Protocols for Security Part 3: Vulnerability Assessment extension for TVRA".

[i.8] ETSI ETR 266: "Methods for Testing and Specification (MTS); Test Purpose style guide".

[i.9] Common Criteria CEM-2001/0015R: "Common Methodology for Information Technology Security Evaluation Part 2: Evaluation Methodology", Supplement: ALC_FLR - Flaw Remediation.

[i.10] ETSI TS 103 486: "CYBER; Identity Management and Discovery for IoT".

[i.11] NIST SP 800-63B: "Digital Identity Guidelines Authentication and Lifecycle Management".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI ES 202 553 [3] apply.

3.2 Symbols

Void.

3.3 Abbreviations

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

AC	Access Control
CC	Common Criteria
CIA	Confidentiality Integrity Availability
DPIA	Data Protection Impact Assessment
EAL	Evaluation Assurance Level
ECC	Error Correcting Code
EUCC	EU Common Criteria Certification Scheme
FIPS	Federal Information Processing Standard
GDPR	General Data Protection Regulation

HW Hardware
ICS Implementation Conformance Statement
ICV Integrity Check Value
IUT Implementation Under Test
L2TP Layer 2 Tunneling Protocol
MAC Message Authentication Code
OAN Optical Access Network
OLT Optical Line Terminal
ON Optical Network
OND Optical Network Device
ONDS Optical Network Device Security
ONDS-M Optical Network Device Security - Management entity
OTN Optical Transport Network
PICS Protocol ICS
PP Protection Profile
RAM Random Access Memory
RoT Root of Trust
RTS Root of Trust for Storage
RtS Root of Trust for Storage
RTV Root of Trust for Verification
SAR Security Assurance Requirement

NOTE: From CCMB-2022-11-002 [8].

SBOM Software Bill of Materials
SFR Security Functional Requirement

NOTE: From CCMB-2022-11-002 [8].

TOE Target of Evaluation
TP Test Purpose
TSF TOE Security Function
TSS Test Suite Structure
TVP Time Variant Parameter
TVRA Threat Vulnerability Risk Analysis
VPN Virtual Private Network

4 Review of base standard

As outlined in each of ETSI TS 103 962 [1] and ETSI TS 103 963 [2], Table 1 identifies, for each statement of the PICS in ETSI TS 103 962 [1] and ETSI TS 103 963 [2], the nature of the test to verify conformance to the requirement. Where conformance can be verified by an automated test to identify a pass or fail verdict the PICS statement is labelled as "conformance". In the case that conformance to the requirement cannot be determined by an automated test, but rather would require examination of design documentation, some form of open box testing, or some other form of expert evaluation, the PICS statement is labelled as "evaluation".

Table 1: Assessment of test mode for each PICS statement from ETSI TS 103 962 [1] and ETSI TS 103 963 [2]

Item	Requirement	Status	Evaluation/ Conformance
Req-1	An access device shall distinguish and keep separate the user and network domains in the device.	M	Evaluation
Req-2	ON systems shall be designed to be secure by default and to support the functionality required by the CIA paradigm.	M	Evaluation
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	Conformance
Req-4	Any link enabled during, and post-initialization, shall support periodic re-establishment of the security association.	M	Conformance
Req-5	The principles of least privilege and least persistence shall apply to all security associations.	M	Evaluation Conformance

Item	Requirement	Status	Evaluation/ Conformance
Req-6	In accordance with the least persistence principle security associations shall not be maintained for longer than required.	M	Evaluation
Req-7	If any software verification fails that software and any supporting elements shall not participate in any security association.	M	Conformance
Req-8	All ON entities shall be able to report the form of CIA protections that are available and operational to authorized entities.	M	Conformance (management)
Req-9	An OAN device shall be integrated to the wider ON and telecommunications system of which it is a component.	M	Evaluation
Req-10	An OAN device shall consist of at least 1 (one) execution environment.	M	Evaluation
Req-11	An OAN device's execution environment shall have 1 (one) initial root of trust.	M	Evaluation
Req-12	The execution environment shall have at least one executable code block.	M	Evaluation
Req-13	There should be a discrete execution environment for each side and discrete roots of trust for each side.	R	Evaluation
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	Evaluation (conformance (see note 1))
Req-15	The OAN Device shall have a root of trust used for initialisation to enable secure boot capabilities.	M	Evaluation
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	Evaluation (see note 2)
Req-17	The guidelines given in NIST SP 800-164 [i.3] 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	Evaluation
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	Evaluation
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	Evaluation
Req-20	The presence of the hardware root of trust shall be asserted by a platform specific attribute certificate.	M	Evaluation Conformance (management (see note 3))
Req-21	All cryptographic modules shall be designed to be crypto-agile.	M	Conformance
Req-22	The specific cryptographic algorithms for each security association shall be defined by the security policy.	M	Conformance
Req-23	Cryptographic algorithms should be sufficient to inhibit known cryptanalysis attacks and mechanisms.	R	Evaluation
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	Evaluation
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	Conformance
Req-26	All ON devices shall be identified with a canonical/root identity and, optionally, additional semantic identifiers identifying their functional nature.	M	Conformance
Req-27	Where provided, the semantic identifier shall be used to indicate the functional nature of the entity.	M C	Conformance
Req-28	The attestation of function shall be verifiable by reference to a 3rd party.	M	Conformance
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	Conformance
Req-30	The to be authenticated identity shall be an attribute of the authentication protocol.	M	Conformance
Req-31	The identity shall always be authenticated on first presentation and periodically thereafter.	M	Conformance
Req-32	In order to be consistent with the principle of least persistence an authenticated session shall expire after a set time.	M	Evaluation Conformance (see note 4)

Item	Requirement	Status	Evaluation/ Conformance
Req-33	The length of an authentication session shall be set by the Authentication-Session-Time-Limit variable.	M	Conformance
Req-34	The Authentication-Session-Time-Limit variable shall be established for each security association.	M	Conformance
Req-35	A device shall be identified in order to be admitted to the operator's trust domain.	M	Conformance
Req-36	Within the trust domain the trust domain manager shall verify the capability of each device.	M	Conformance
Req-37	An ON device shall present an identifier to each of the client and the network side of the device.	M	Conformance Evaluation (see note 12)
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	Evaluation (see note 5)
Req-39	Any identifier presented by the device shall be authenticated by the receiving device.	M	Conformance
Req-40	A key shall be associated to an attribute or identifier of the OAN Device.	M	Conformance
Req-41	The binding of key to the attribute or identifier shall be maintained for each security association.	M	Conformance
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	Conformance
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	Conformance Evaluation (note 6)
Req-44	The MAC approach to authentication as outlined in ETSI TS 102 165-2 [6] shall apply.	M	Evaluation
Req-45	Random challenges used in any MAC based authentication shall be generated using a true source of randomness.	M	Evaluation
Req-46	Software only functions shall not be used to generate random challenges.	M	Evaluation
Req-47	A challenge-response method should be used at initialisation and for key establishment, key refresh, events.	R	Evaluation
Req-48	Only cryptographically relevant challenge response schemes shall be used.	M	Evaluation
Req-49	The challenge response approach to authentication as outlined in ETSI TS 102 165-2 [6] shall apply.	M	Evaluation
Req-50	Random challenges used in any challenge-response protocol shall be generated using a true source of randomness.	M	Evaluation
Req-51	A device should only be able to perform a self-attestation of its identity at initialisation.	R	Evaluation
Req-52	The self-attestation shall be provided in the form of a digital signature and include a signed public key.	M C	Conformance
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	Evaluation (see note 7)
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	Evaluation
Req-55	The OAN device shall have a root of trust for storage to store private cryptographic material (private key).	M	Evaluation (see note 7)
Req-56	In accordance with ETSI TS 103 486 [i.10] the identity (canonical) and identifying attributes of a device should be attested to by an appropriate independent 3rd party.	R	Conformance
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	Conformance
Req-58	A device should only be able to perform a self-attestation of its capability at initialisation.	R C	Evaluation
Req-59	The self-attestation shall be provided in the form of a digital signature and include a self-signed public key.	M C	Conformance

Item	Requirement	Status	Evaluation/ Conformance
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	Conformance
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	Conformance
Req-62	All exchanged discrete messages shall have their integrity verified on reception at the device.	M	Conformance
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	Evaluation
Req-64	Any message that fails the integrity check shall be discarded and an error reported.	M	Conformance
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	Conformance
Req-66	All transmissions made from the OLT towards the network should be protected by a confidentiality security association.	R	Conformance
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	Conformance
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	Evaluation (see note 8) Conformance
Req-69	Every access device shall have a root of trust for storage (RtS).	M	Evaluation (see notes 1 and 2)
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	Evaluation
Req-71	All data in OAN devices shall be made available to authorized entities using the principle of least privilege.	M	Conformance (see note 9)
Req-72	The access control mechanism shall follow the policy model outlined in ETSI TS 102 165-2 [6].	M	Evaluation
Req-73	Each protected Object in the OAN device shall be protected by an access control policy.	M	Evaluation (see note 10)
Req-74	The access control policy shall be evaluated on each access attempt.	M	Conformance
Req-75	The policy shall consist of 1 or more rules each of which shall be evaluated in turn.	M	Conformance
Req-76	Every denied access attempt shall be recorded.	M	Conformance
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	Conformance

Item	Requirement	Status	Evaluation/ Conformance
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	Conformance
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	Conformance
Req-80	If an exception is raised it shall include the details of the rule that failed.	M	Conformance
Req-81	The default access control condition for all objects shall be "do not allow"/"do not permit".	M	Conformance
Req-82	The following rules shall be implemented in OAN devices: CFG-AC; CK-AC; DEV-AC; PAC-AC. The rules are detailed in ETSI TS 103 962 [1]	M	Conformance (see note 11)
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	Conformance
Req-84	A policy shall only set access control permission to True where all rules of any policy pass	M	Conformance

NOTE 1: For Req-14 where it is required to demonstrate physical and cryptographic separation of distinct clients in the case of a multi-occupancy client environment it may be necessary to evaluate the design documentation to assess that the capability exists and also perform automated conformance tests to verify the underlying function.
NOTE 2: For Req-16 the existence of the root of trust and where it is applied shall be verified against the design documentation which shall clearly identify when it is invoked and for what purpose.
NOTE 3: For Req-20 the presence of the hardware root of trust may also be verified by demonstration of conformance to an evaluated PP for the root of trust.
NOTE 4: In Req-32 the rationale for the expiry time and its justification is expected to be subject to review of the design documentation and the actual behaviour tested in an automated conformance test.
NOTE 5: Req-38 asks that it should not be feasible to determine/infer the identifier presented to one side from knowledge of the identifier presented to the other side which may be demonstrated by examination of the design documentation that should illustrate the analysis that gives confidence the requirement is met.
NOTE 6: In Req-43 the design documentation should make clear where a MAC is applied (the evaluation element of the test) and a conformance test can be used to verify the MAC operation.
NOTE 7: For Req-53 this is an application of the RoT identified in Req-16 and Req-20.
NOTE 8: Req-68 requires evaluation of the design documentation to validate the use of the chosen encryption mode and then conformance tests can be used to verify the operation.
NOTE 9: For Req-71 conformance tests of the access control protocol and associated policies is expected.
NOTE 10: For Req-73 the design documentation shall make clear what is addressed by the access control policy.
NOTE 11: Req-82 requires that the specific rules are transposed to the access control model that is implemented.
NOTE 12: Req-37 applies only for OAN devices, OTN devices do not present their identity to clients.

5 Test suite structure

The test suite structure is defined using TPLan (see ETSI ES 202 553 [3]).

The TSS header shall be as below:

```
TSS     : ONDS_TSS
title   : 'TSS&TP for testing of ETSI TS 103 962 and TS 103 963'
version : 1.0
date    : xx.yy.2025    -- could also be written as xx/yy/2025 or xx-yy-2025
author  : 'ETSI TC CYBER'
```

Given the nature of security testing where in certain cases an absolute pass or fail judgement can be difficult to assign, the analysis identifies, for each test purpose, the evaluation criteria that applies in order to provide a pass or fail assignment. The terminology of Common Criteria Part 2 [8] is applied and the extension and application of TPLan that applies for the SFRs from Common Criteria that apply to the present document is given in Annex A.

The base standards for the purpose of the present document are defined using the **xref** keyword as below.

```
xref BaseStandards {TS1103962, TS103963}
```

Tests are grouped for the purposes of the present document using the structure of ETSI TS 103 962 [1] and ETSI TS 103 963 [2] as a guide and identified as follows:

1) Identification and authentication
2) Confidentiality and integrity protection of data transfer
3) Access control
4) Device provisions

The further classification of tests into sub-groups follow the general classification in [1] and [2] for those requirements identified as "Conformance" in Table 1. A second set of groups and sub-groups is identified for the same broad groupings to address those requirements identified in Table 1 as "Evaluation".

These groups and associated sub-groups are identified using TPLan as below and are specified for convenience of the tester.

Group 1 addresses requirements 26 to 31, 33 to 37, 39 to 43, 52, 56-57, and 59-61 of [1] and [2].

```
group 1 'Identification and authentication'
objective 'Verification of requirements from Clause 5 of xref'
end group 1 'Identification and authentication'
```

Group 2 addresses requirements 62 and 64-67 of [1] and [2].

```
group 2 'Confidentiality and integrity protection of data transfer'
objective 'Verification of requirements from Clause 6 of xref'
end group 2 'Confidentiality and integrity protection of data transfer'
```

Group 3 addresses requirements 3-4, 7-8, 21-22 and 25 of [1] and [2].

```
group 3 'Access control'
objective 'Verification of requirements from Clause 7 of xref'
end group 1 'Access control'
```

Group 4 addresses requirements … of [1] and [2].

```
group 4 'Device provisions'
objective 'Verification of requirements from Clause 4 of xref'
end group 4 'Device provisions'
```

Group 5 addresses those requirements identified in Table 1 as for "evaluation" and identify additional test purposes mapped to the Common Criteria (CC) Security Functional Requirements (SFRs) as outlined in Annex A.

```
group 5 'Evaluation provisions'
objective 'Verification of those requirements from xref that are marked for evaluation'
end group 5 'Evaluation provisions'
```

6 Test purposes

6.1 Overview

Each test purpose examines a requirement and identifies the objective of the test (written in the summary field), the particular requirement(s) that are being tested, and the configuration necessary to conduct the test.

As outlined in ETSI ES 202 553 [3] each test is described by any necessary configuration and preconditions, and a series of stimuli and responses. Where extensions to TPLan are made as in the present clause these are added to the header (see ETSI ES 202 553 [3], clause C.2.3).

6.2 Configurations, keywords and preconditions

Many of the requirements identified in ETSI TS 103 962 [1] and ETSI TS 103 963 [2] can be summarized as providing preconditions within the test configuration. Thus the following requirements are identified as preconditions using the keyword "with":

```
with {IUT 'having a canonical identifier'} -- Req-26
with {IUT 'having a semantic identifier'} -- Req-27
with {IUT 'having a semantic identifier attested to by a 3rd party'} -- Req-28
with {IUT 'set a non-zero value for the Authentication-Session-Time-Limit variable'} -- Req-33
with {IUT 'having at least 1 (one) execution environment'} -- Req-10, Req-12
with {IUT 'having discrete execution environments for client and network'} -- Req-13
with {IUT 'having 1 initial root of trust'} -- Req-11, Req-16, Req-18, Req-19, Req-20
with {IUT 'having a root of trust to enable secure boot'} -- Req-15
with {IUT 'having a hardware based root of trust'} -- Req-54, Req-17
with {IUT 'having the root of trust for storage and verification'} -- Req-69, Req-70, Req-55
with {IUT 'having crypto-agile cryptographic modules'} -- Req-21
with {IUT 'having proof of presence of hardware root of trust'} -- Req-20
with {IUT 'having cryptographic algorithms robust against known cryptanalysis'} -- Req-23,
with {IUT 'having a cryptographic key generation algorithm'} -- Req-53
with {IUT 'having generated a true random element'} - Req-45, 50, -54
with {IUT 'having a random value generator not based only on software'} -- Req-46
with {IUT 'having been designed to be secure by default'} -- Req-2
with {IUT 'having physical and cryptographic separation of tenants'} -- Req-1, Req-14
```

NOTE 1: Many other requirements may be satisfied by a combination of one or more of the above pre-conditions, for example Req-9 is satisfied by a combination of the requirements related to execution environment and the establishment of security associations (see clause 6.3.1).

The following states are defined as conditions:

```
def condition NotIdentified, Identified, NotAuthenticated, Authenticated
def condition InAuthenticationSession
```

The following timers and values are defined in order to ensure the principle of least persistence (Req-3, Req-5, Req-6) can be tested (these timers also satisfy Req-32, Req-33, and Req-34 (time limit) and each of Req-76, Req-78 and Req-81 (failure limit)):

```
def value AuthenticationSessionTimeLimit '600' – Default value of authentication session in seconds
def value AuthenticationAttemptFailureLimit '3' - Default value for number of allowed auth fails
def value AccessAttemptFailureLimit '3' - Default value for number of allowed access control fails
def value UserInactivityTimeLimit '120' - Default value of inactivity timeout in seconds
def value AccessControl {Permit|Deny}'Deny' -- Default is that access is denied (Req-81)
def value SecurityAssociationTimeLimit '120' -- (Req-6)
```

NOTE 2: There is no defined value for the session time limit in [1] and [2], thus the value selected here is for testing purposes only.

NOTE 3: There is no defined value for the number of times an access control or authentication attempt failure is tolerated [1] and [2], thus the value selected here is for testing purposes only.

The following keywords are defined for the access control capabilities.

```
def word verifies -- used when verifying, for example, an integrity check value
def word discards -- used when a test or condition fails and no further processing is performed
def word permit -- when access control determins that access is allowed
def word deny -- when access control determins that access is not allowed
def word encrypts -- for use in cases where content is encrypted by the IUT
def word decrypts -- for use in cases where content is decrypted by the IUT
def word evaluates -- used to test an access control policy or rule
def word expires -- used to identify a timer has expired
```

Where authentication is achieved by an exchange of messages the message shall contain the to be authenticated identity (Req-30).

```
def event authentication-request -- For challenge response authentication (Req-45 through Req-50)
def event authentication-response -- For challenge response authentication (Req-45 through Req-50)
def event authentication-claim {} -- used to assert an identity (Req-43, Req-44)
def event authentication-verification -- for verifying that authentication has succeeded
```

Many SFRs as described in Common Criteria Part 2 [i.4] are not easily mapped to the stimulus-response model of TPLan and the following additional header elements are defined to enable such a mapping to make sense by defining states that identify the pre- and post- conditions for the application of the identified SFRs.

```
def event auditable-event-notification -- Used for Functional Class FAU (Security Audit)
def event auditable-event-response -- Used for Functional Class FAU (Security Audit)
```

6.3 Test purposes per group

6.3.1 Identification and authentication

TP Id	ONDS-IA-001
Test Objective	The identity shall always be authenticated on first presentation and periodically thereafter (the latter also is used to verify the operation of periodic re-establishment of a security association (here for authentication))
Reference	REQ-31, REQ-30, REQ-4, REQ-8 (implicit), REQ-22, REQ-29
Configuration	
PICS Selection	
Initial conditions	
with {**IUT in** NotIdentified **and** NotAuthenticated} with {IUT 'having relevant algorithms and key formats defined in the security policy}	
Expected behaviour	

ensure that {
  when {**IUT receives** 'Startup' or 'Reauthentication timer expires'}
  then [**IUT sends** authentication-claim **containing** 'semantic or canonical identifier'}
  when {**IUT receives** authentication-verification}
  then {**IUT in** Authenticated **and** Identified}
}	

NOTE: Requirement 8, that requires the reporting of the form of CIA protections is implicit in TP ONDA-IA-001.

6.3.2 Confidentiality and integrity protection of data transfer

TP Id	ONDS-CI-001
Test Objective	Verify that inbound messages contain an Integrity Check Value (ICV) that is tested for correctness whilst the authentication period is still valid
Reference	REQ-62, REQ-65
Configuration	
PICS Selection	
Initial conditions	
with {**IUT in** Identified **and** Authenticated} -- verifies that authentication period is valid	
Expected behaviour	

ensure that {
  when {**the IUT receives** 'any message'
  containing 'ICV'
  and containing 'TVP'}
  then {**the IUT generates** 'calculated-ICV'} – gives 'calculated-ICV'
  when {**the IUT verifies** 'calculated-ICV' **is equal to** 'ICV'}
  then {**the IUT permits** 'any message'}
}	

TP Id	ONDS-CI-002
Test Objective	Verify that inbound messages contain an Integrity Check Value (ICV) that is tested for correctness whilst the authentication period is still valid and is discarded on ICV failure and an alert raised
Reference	REQ-64
Configuration	
PICS Selection	
Initial conditions	
with {**IUT in** Identified **and** Authenticated} -- verifies that authentication period is valid	

Expected behaviour

ensure that {
when {**the IUT receives** 'any message' **containing** 'ICV' **and containing** 'TVP'}
then {**the IUT generates** 'calculated-ICV'}
when {**the IUT verifies** 'calculated-ICV' **is not equal to** 'ICV'}
then {**the IUT discards** 'any message' **and the IUT reports** 'ICV verification error'}
}

TP Id	ONDS-CI-003
Test Objective	Verify that messages made from the OLT are protected by a confidentiality security association
Reference	REQ-66
Configuration	
PICS Selection	
Initial conditions	
with {**IUT in** Identified **and** Authenticated} -- verifies that authentication period is valid	
Expected behaviour	

ensure that {
when {the IUT sends 'any message'}
then {the IUT encrypts 'any message'}
}	

6.3.3 Access control

TP Id	ONDS-AC-001
Test Objective	Evaluate access control policy on each access attempt
Reference	REQ-74, REQ-82 (implicit)
Configuration	
PICS Selection	
Initial conditions	
with {**IUT in** Identified **and** Authenticated} -- verifies that authentication period is valid	
Expected behaviour	

ensure that {
when {IUT configuration-data is accessed}
then {IUT evaluates 'if policy conditions are met'}
when {evaluation is true}
then {PERMIT}
}	

TP Id	ONDS-AC-002
Test Objective	Record failed access attempt
Reference	REQ-76, REQ-77, REQ-79, REQ-80, REQ-82 (implicit)
Configuration	
PICS Selection	
Initial conditions	
with {**IUT in** Identified **and** Authenticated} -- verifies that authentication period is valid	
Expected behaviour	

ensure that {
when {IUT configuration-data is accessed}
then {IUT evaluates 'if policy conditions are met'}
when {evaluation is false}
then {DENY and Record-access-control-error and 'Record rule that caused the error'}
}	

TP Id	ONDS-AC-003
Test Objective	Verify that all access control rules are tested and pass to allow access control as Permit
Reference	REQ-75, REQ-83, REQ-84
Configuration	
PICS Selection	
Initial conditions	
with {IUT in Identified and Authenticated and AccessControl is Deny}	
Expected behaviour	

ensure that {
when {IUT 'protected data' is accessed and 'policy contains n rules'}
then {IUT evaluates 'rule 1' and 'rule 2' and … 'rule n'}
when {evaluation is true}
then {set AccessControl to Permit}
}	

6.3.4 Device provisions

TP Id	ONDS-DEV-001
Test Objective	If any software verification fails ensure that that software and any supporting elements shall not participate in any security association
Reference	REQ-7
Configuration	
PICS Selection	
Initial conditions	
with {IUT in Identified and Authenticated and AccessControl is Deny}	
Expected behaviour	

ensure that {
when {IUT 'protected data' is accessed and 'policy contains n rules'}
then {IUT evaluates 'rule 1' and 'rule 2' and … 'rule n'}
when {evaluation is true}
then {set AccessContol to Permit}
}	

TP Id	ONDS-DEV-002
Test Objective	To verify secure boot uses a root of trust
Reference	REQ-7
Configuration	
PICS Selection	
Initial conditions	
with {IUT in Identified and Authenticated and AccessControl is Deny}	
Expected behaviour	

ensure that {
when {IUT 'protected data' is accessed and 'policy contains n rules'}
then {IUT evaluates 'rule 1' and 'rule 2' and … 'rule n'}
when {evaluation is true}
then {set AccessControl to Permit}
}	

6.3.5 Evaluation provisions

The majority of test purposes for requirements identified as for "evaluation" are defined as pre-conditions in clause 6.2. A small number of the "evaluation" requirements can only be assessed by detailed evaluation of the design documents (as identified in several requirements).

In all cases the TPLan outlines given in the present document should be addressed by the evaluator alongside the guidance given in Common Criteria for Information Technology, Evaluation Methodology [7].

Annex A (normative): TPLan extensions for ONDS and Common Criteria

A.1 SFR structure

The following SFR modules are identified as applicable to the present document from ETSI TS 103 962 [1] and ETSI TS 103 963 [2] and given in ETSI TS 103 996 [i.4]:

- FAU_GEN.1.2 Audit data generation
- FCS_CKM.1.1 Cryptographic key generation
- FCS_CKM.2 Cryptographic key distribution
- FCS_CKM.3 Cryptographic key access
- FCS_CKM.6 Timing and event of cryptographic key destruction
- FCS_COP.1.1 Cryptographic operation
- FCS_RNG.1 Generation of random numbers
- FDP_ACC.1 Subset Access Control
- FDP_ACF.1 Security attribute based access control
- FDP_SDC.1 Stored data confidentiality
- FDP_SDI.1.1 Stored data integrity monitoring
- FIA_AFL.1 Authentication failure handling
- FIA_API.1 Authentication proof of identity
- FIA_ATD.1 User attribute definition
- FIA_UAU.1 Timing of authentication
- FIA_UID.1 Timing of identification
- FMT_MSA.1 Management of security attributes
- FMT_MSA.3 Static attribute initialization
- FMT_SMR.1 Security roles
- FMT_SMF.1 Specification of Management Functions
- FPT_HWROT.1 Root of trust based on HW
- FPT_INI.1 TSF initialization
- FTA_SSL.3 TSF-initiated termination
- FTP_ITC.1 - Inter-TSF trusted channel

Each SFR from CC gives guidance on how the requirement is to be evaluated. This evaluation is addressed as a test purpose in the present document, and the present annex creates a template TPLan structure for each SFR that can be applied for the main body of the present document.

NOTE: The full TPLan structure is not shown as the set of header elements is taken from those identified in clause 6 or as shown in clause A.2 of the present document.

A.2 Application of TSS&TP styles to SFRs from ETSI TS 103 996

A.2.0 Note

Where no specific TPLan assessment is given the provisions of Common Criteria for Information Technology, Evaluation Methodology [7] apply.

A.2.1 FAU_GEN.1.2 Audit data generation

As described in ETSI TS 103 996 [i.4] the SFR FAU_GEN.1.2 is intended to satisfy requirements 76, 77 and 80 from ETSI TS 103 962 [1] and ETSI TS 103 963 [2]. It is the IUT that is tested and the TSF within the IUT that is implicitly tested. Thus in general terms for the IUT as specified in [1] and [2] and where FAU_GEN.1.2 is used (with FAU_GEN.1.1 implied):

```
ensure that {
    when {IUT receives 'audit-function-started'
            or 'audit-function-stopped'
            or any-event in 'detailed auditable event'
            or 'FW-update'
            or 'SW-update'
            or 'access attempt to log record'
            or 'access to TEI management'}
    then {IUT generates 'detailed audit record'} -- SFR_FAU_GEN.1.2
}
```

The above is also addressed in the access control test purposes given in clause 6.3.3 of the present document.

A.2.2 FCS_CKM.1.1 Cryptographic key generation

As described in ETSI TS 103 996 [i.4] the SFR FCS_CKM.1.1 is intended to satisfy requirements 24, 41 and 52 from ETSI TS 103 962 [1] and ETSI TS 103 963 [2]. As stated in [i.4] no specific cryptographic provisions are made but rather ask that the OND implementer refers to best practice, as in Annex D of ETSI TS 103 924 [4]. For this the tester has to be able to deliver a stimulus that requires the IUT to generate a cryptographic key that can be shown to have been generated only by the key generation algorithm claimed by the implementation.

```
with {IUT 'having a cryptographic key generation algorithm'}

ensure that {
    when {IUT receives 'cryptographic key generation request'}
    then {IUT generates 'key in accordance with a specified cryptographic key generation algorithm'}
}
```

A.2.3 FCS_CKM.2 Cryptographic key distribution

As described in ETSI TS 103 996 [i.4] the SFR FCS_CKM.2 is intended to satisfy requirement 52 from ETSI TS 103 962 [1] and ETSI TS 103 963 [2]. As for clause A.2.2, it is stated in [i.4] that no specific cryptographic provisions are made but rather ask that the OND implementer refers to best practice, as in Annex D of ETSI TS 103 924 [4]. For this the tester has to be able to deliver a stimulus that requires the IUT to distribute a cryptographic key that can be shown to have been distributed only by the key distribution method claimed by the implementation.

```
with {IUT 'having a cryptographic key distribution mechanism'}
ensure that {
    when {IUT receives 'cryptographic key distribution request'}
    then {IUT sends 'key in accordance with a specified cryptographic key distribution mechanism'}
}
```

A.2.4 FCS_CKM.3 Cryptographic key access

As defined in ETSI TS 103 996 [i.4] the SFR FCS_CKM.3 is intended to satisfy all the requirements identified in ETSI TS 103 962 [1] and ETSI TS 103 963 [2] that require a cryptographic keyed operation outside of the TOE. As stated in [i.4] best practice is followed wherein keys are only made available to the function requiring them and are not available by any other mechanism. However it is also noted in the application notes of CC Part 2 [8] that this component is intended to allow the specification of requirements on the usage of keys outside the TOE (e.g. backup, archival, escrow, recovery) which are not supported by [1] and [2].

NOTE: FCS_CKM.3 does not intend to describe the key management or access to keys on the TOE.

A.2.5 FCS_CKM.6 Timing and event of cryptographic key destruction

In best practice whenever a key is no longer in use it should be destroyed. This is stated in the SFR from CC Part 2 [8] as "The TSF shall destroy [assignment: list of cryptographic keys (including keying material)] when [selection: no longer needed, [assignment: other circumstances for key or keying material destruction]]."

```
ensure that {
    when {IUT receives 'destroy cryptographic keys command' containing 'Key-id'}
    then {IUT destroys 'all material identified by Key-id'}
}
```

A.2.6 FCS_COP.1.1 Cryptographic operation

In CC Part 2 [8] the SFR is stated as "The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards]." However, in ETSI TS 103 996 [i.4] it is stated that "The base requirements do not specify cryptographic algorithms or key sizes, but rather refer to best practice". Thus for testing purposes the following preconditions are defined including references to a number of FIPS documents that define commonly used cryptographic algorithms.

```
with {IUT 'having an algorithm for authentication'}
with {IUT 'having an algorithm for producing an integrity check value'}
with {IUT 'having an algorithm for encryption'}
with {IUT 'having an algorithm for decryption'}
with {IUT 'having an algorithm for signature creation'}
with {IUT 'having an algorithm for singature verification'}

def value SymmetricKeySize '128'
def value AsymmetricKeySize-ECC '256' -- for equivalence to 128-bit symmetric key
def value AsymmetricKeySize-RSA '3072' -- for equivalence to 128-bit symmetric key
xref CryptoStandards {FIPS197, FIPS180-4, FIPS186-4, FPIS186-5}
```

A.2.7 FCS_RNG.1 Generation of random numbers

As identified in ETSI TS 103 996 [i.4] the generation of random numbers is required by the OND having a physical or non-physical-true or deterministic random number generator. This is addressed using TPLan by defining the following pre-conditions.

```
with {IUT 'having a physical random number generator'}
with {IUT 'having a deterministic random number generator'}
```

A.2.8 FDP_ACC.1 Subset Access Control

For ONDs the access control test purposes are defined in clause 6.3.3 of the present document.

A.2.9 FDP_ACF.1 Security attribute based access control

The model identified in ETSI TS 103 962 [1] and ETSI TS 103 963 [2], and declared in ETSI TS 103 996 [i.4], is policy and attribute based access control.

A.2.10 FDP_SDC.1 Stored data confidentiality

As identified in ETSI TS 103 996 [i.4] all sensitive user data is expected to be confidential while it is stored in persistent memory. This is addressed by TPLan as a set of pre-conditions given below.

```
with {IUT 'having password stored in a manner consistent with clause 5.1.1 of NIST SP 800-63B'}
with {IUT 'having sensitive user data stored confidentiality in persistent memory'}
```

A.2.11 FDP_SDI.1.1 Stored data integrity monitoring

As defined in CC Part 2 [8] and for the requirements identified in ETSI TS 103 996 [i.4] it is expected that the memory used for data storage is able to identify, report, and ideally, correct integrity errors arising from accidental (unintentional) errors (e.g. hardware glitches). This is addressed by defining the following TPLan pre-condition.

```
with {IUT 'having memory for user data storage capable of identifying integrity errors'}
```

NOTE 1: The wording in CC Part 2 [8] uses the term "monitor for integrity errors" which is interpreted for the present document as having the meaning of "identify integrity errors" as monitoring is an implicit action in being able to identify.

NOTE 2: Error Correcting Code (ECC) memory chips can be used to automatically correct errors in RAM by generating Hamming Codes of the memory entry and, if used, may claim to meet the identified pre-condition.

A.2.12 FIA_AFL.1 Authentication failure handling

The general assumption in the present document and in ETSI TS 103 962 [1] and ETSI TS 103 963 [2] is that a common failure handling mechanism is applied across the OND. This is specifically handled for ONDs using the test purposes identified in clause 6.3.1 of the present document and by the defined constant defined in clause 6.2.

A.2.13 FIA_API.1 Authentication proof of identity

The CC Part 2 [8] statement requires that the TSF provide an authentication mechanism to prove the identity of an entity by including a ***list of properties*** to an external entity. In TPLan this is addressed by requiring specific elements in the authentication messages (see clause 6.2). The following TPLan elements are indicative.

```
ensure that {
    when {IUT receives authentication-request containing 'property in list of properties'}
    …
}
```

A.2.14 FIA_ATD.1 User attribute definition

In CC Part 2 [8] the behaviour of FIA_ATD.1 requires that the TSF maintains a list of the security attributes belonging to individual users. For the present document where attribute based access control is considered then the rules defined as part of ONDS-AC-003 apply.

A.2.15 FIA_UAU.1 Timing of authentication

In CC Part 2 [8] the description of the behaviour of FIA_UAU.1 is that the TSF shall allow only some, listed, TSF-mediated actions on behalf of the user to be performed before the user is authenticated. The test purpose therefore shall be written in such a way that both positive and negative behaviour can be assessed, i.e. test that each allowed action is permitted, and that any other action is denied.

NOTE: This is addressed specifically for the OND case in clause 6.3.1 of the present document.

It is reasonable to model the allowed actions as part of the access control policy and then to have authentication as an attribute of certain access control rules. In doing this the provisions and tests of clause 6.3.3 apply (see also clause A.2.16 for the similar case of actions before identification).

TP Id	
Test Objective	To verify that only listed actions are allowed to be performed before the user is authenticated
Reference	FIA_UAU.1 Timing of authentication from CC Part 2 [8]
Configuration	
PICS Selection	
Initial conditions	
with {**IUT in** NotAuthenticated }	
Expected behaviour	

ensure that {
when {**IUT receives** 'any event'}
then {IUT evaluates 'if policy conditions are met'}
when {evaluation is true}
then {PERMIT}
}	

A.2.16 FIA_UID.1 Timing of identification

In CC Part 2 [8] the description of the behaviour of FIA_UID.1 is that the TSF shall allow only some, listed, TSF-mediated actions on behalf of the user to be performed before the user is identified. The test purpose therefore shall be written in such a way that both positive and negative behaviour can be assessed, i.e. test that each allowed action is permitted, and that any other action is denied.

NOTE: This is addressed specifically for the OND case in clause 6.3.1 of the present document.

It is reasonable to model the allowed actions as part of the access control policy and to have identification as an attribute of certain access control rules. In doing this the provisions and tests of clause 6.3.3 apply.

TP Id	
Test Objective	To verify that only listed actions are allowed to be performed before the user is identified
Reference	FIA_UID.1 Timing of identification from CC Part 2 [8]
Configuration	
PICS Selection	
Initial conditions	
with {**IUT in** NotIdentified }	
Expected behaviour	

ensure that {
when {**IUT receives** 'any event'}
then {IUT evaluates 'if policy conditions are met'}
when {evaluation is true}
then {PERMIT}
}	

A.2.17 FMT_MSA.1 Management of security attributes

As per CC Part 2 [8] it is recognized that FMT_MSA.1 is addressed by the access control policy where the "security attributes" are specific assets to which access is restricted (see clause 6.3.3 of the present document).

A.2.18 FMT_MSA.3 Static attribute initialization

Whilst CC Part 2 [8] states that the purpose of this SFR is to strictly control security attributes this is within the overall access control suite identified for the present document by the test purposes in clause 6.3.3. For the more general application of this SFR in which is it intended to verify that the default values of security attributes are appropriately either permissive or restrictive in nature the following pre-conditions apply and test purposes apply.

NOTE: Restrictive attributes are those where only values specifically allowed by the application are permitted, any other value is denied. Permissive attributes are those whose allowed values are set by the specific context.

EXAMPLE 1: If an attribute value can take only the values 1,3 and 5 then it is possible to test for permit for only those values and to confirm that deny is true for any other value.

EXAMPLE 2: If an attribute can take a range of values it is determined as permissive and testing should address a sufficient number of values in the range, at the limits of the range, and outside the limits of the range to determine correct behaviour.

```
with {IUT 'having attributes used in access control being restrictive'}
ensure that {
    when {IUT receives 'access control request' containing 'attribute'}
    then [IUT verifies 'attribute' is 'restrictive'}
}

with {IUT 'having attributes used in access control being permissive'}
ensure that {
    when {IUT receives 'access control request' containing 'attribute'}
    then [IUT verifies 'attribute' is 'permissive'}
}
```

A.2.19 FMT_SMR.1 Security roles

Roles are defined as states that can be measured and upon which actions can be taken.

```
def condition Administrator, User -- FMT_SMR.1.1
def value user_roles {'list of allowed user actions'} -- FMT_SMR.1.2
def value admin_roles {'list of allowed administrator actions'} -- FMT_SMR.1.2
```

NOTE: It is expected that in addition to the roles themselves that the system will map assets (functions, access control conditions to data, and so forth) to each role which is seen in the list of values given above.

EXAMPLE: An access control rule may include statements such as "if role is user then permit user action".

A.2.20 FMT_SMF.1 Specification of Management Functions

In CC Part 2 [8] each SFR has an identified management function (e.g. for FAI_UAU.1 the expected management functions are to establish the threshold for authentication failures and to define the actions to be taken in the event of authentication failure and these are defined for ONDs in clauses 6.2 and 6.3.1 of the present document). As such the specific test purposes for FMT_SMF.1 are not distinct but form part of each SFR and no specific generalization of this SFR is given.

A.2.21 FPT_HWROT.1 Root of trust based on HW

The base CC Part 2 [8] does not specify FPT_HWROT but it is defined in ETSI TS 103 996 [i.4] as an extension. The intent is that there is a root of trust implemented as immutable HW based module for storing sensitive data. This is addressed in TPLan as a precondition.

```
with {IUT 'having a hardware based root of trust'}
```

See also the set of preconditions given in clause 6.2 of the present document.

A.2.22 FPT_INI.1 TSF initialization

In CC Part 2 [8] the statement for FPT_INI.1 is given as follows "*The TOE shall provide an initialization function which is self-protected for integrity and authenticity*". The broad assumption for the OND case is that the boot software can have its integrity and authenticity verified, which may require that the software is signed and that the signature is verified.

```
with {IUT 'having signed boot image'}
ensure that {
    when {IUT receives 'initialisation request'}
```

```
    then [IUT verifies 'signature of boot image'}
}
```

A.2.23 FTA_SSL.3 TSF-initiated termination

In CC Part 2 [8] the SFR FTA_SSL.3 applies for interactive user sessions and requires that a timer is established for how long such sessions can be inactive (see clause 6.2 of the present document).

```
ensure that {
    when {IUT expires UserInactivityTimeLimit}
    then [IUT closes 'interactive session'}
}
```

NOTE: There is not expected to be significant levels of interactive user sessions in an OND but such sessions may be used for remote configuration and thus form part of the access control rules.

A.2.24 FTP_ITC.1 - Inter-TSF trusted channel

The purpose of FTP_ICT.1 in the context of OND is to ensure that any remote entity is within the trust domain of the OND. This can be implemented using, for example, a VPN protocol such as IPsec or L2TP. In each case the result is that the remote entity and the OND are securely connected where the trusted channel is between known (identified and authenticated) parties, and where any data on the channel is protected from eavesdropping and manipulation.

```
with {IUT 'having a distinct channel to a remote management entity'} -- trusted channel
with {IUT 'having trusted channel encrypted'}
with {IUT 'having trusted channel with integrity protection'}
with {IUT 'having end-points of the trusted channel authenticated'}

ensure that {
    when {IUT receives 'remote connection request from the remote management entity'}
    then {IUT directs 'remote connection to use trusted channel'}
}
```

Annex B (informative): Considerations for the EUCC PP programme

NOTE 1: The mapping given here is indicative and does not claim to be the only mapping that is possible, rather it is a reasonable mapping that aligns the content of the main body of the present document to the essential requirements of the CRA and is intended to show that the PP can be used in any claim of the product that conforms to the PP (the present document) is also conformant to the CRA. It may be possible, and reasonable, for other mappings to be identified.

The text of the present annex maps the suite of test purposes given in the main body of the present document to the expectations of the Cyber Resilience Act [i.1] and of the interpretation of the CRA for substantial and high levels of evaluation defined in the Cyber Security Act [i.3].

NOTE 2: The provisions and recommendations given in ETSI TR 103 866 [i.6] for the application of security controls in the NIS2 domain apply to the ONDS domain.

Table B.1: Essential Cybersecurity requirements relating to the properties of products with digital elements

Id	Text from CRA - Annex I		Test process	Determination
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;		Evaluation of the summary TVRA given in the ONDS requirements catalogue and by reference to any equivalent analysis indicated by the submitting entity. Using the tools from Common Criteria this should include evaluation of the following Security Assurance Requirements: ADV_ARC.1 ALC_CMC.3 ALC_CMS.2 ADV_TDS.1 or ADV_TDS.2 (depending on the EAL claim). See note.	Pass or fail based on the evaluation report.
2	On the basis of the cybersecurity risk assessment referred to in Article 13(2) of Regulation (EU) 2024/2847 [i.1] and where applicable, products with digital elements shall:			
	2a	be made available on the market without known exploitable vulnerabilities;	Evaluation of the design process and by a limited degree of penetration testing consistent with AVA_VAN for the intended market and attacker capability (see ETSI TS 102 165-3 [i.7] for a guide to prepare the penetration test).	Pass or fail based on the evaluation report.
	2b	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;		On the assumption that secure by default is defined then a pass or fail is given based on the evaluation report.
	2c	ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;		
	2d	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;		

Id	Text from CRA - Annex I		Test process	Determination
	2e	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;		
	2f	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;		
	2g	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 (minimisation of data);	This should be documented in a DPIA and also comply to relevant data protection regulation (e.g. GDPR).	Pass or fail based on evaluation of the DPIA and selective sampling of data to ensure non-essential data is rejected.
	2h	protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;	Evaluation of the session termination and the security architecture: FTA_SSL.3 ADV_ARC.1	On the evaluation of the SFR/SAR-results, a pass or fail is given in the evaluation report.
	2i	minimize the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;	Evaluation of the event reporting, the security architecture and the user guidance: FAU_GEN.1 AGD_OPE.1 ADV_ARC.1	On the evaluation of the SFR/SAR-results, a pass or fail is given in the evaluation report.

Id	Text from CRA - Annex I		Test process	Determination
	2j	be designed, developed and produced to limit attack surfaces, including external interfaces;	Evaluation of the security architecture, the design, the functional specification and the vulnerability assessment: ADV_ARC.1 ADV_TDS.2 or ADV_TDS.3 ADV_FSP.3 or ADV_FSP.4 AVA_VAN.2 or AVA_VAN.3	On the evaluation of the SAR-results, a pass or fail is given in the evaluation report.
	2k	be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;	Evaluation of the event reporting, user roles, security architecture, the functional specification: ADV_ARC.1 ADV_TDS.2 or ADV_TDS.3 ADV_FSP.3 or ADV_FSP.4	On the evaluation of the SAR-results, a pass or fail is given in the evaluation report.
	2l	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;	Evaluation of the event reporting, of the management functions and the user roles: FAU_GEN.1 FMT_SMF.1 FMT_SMR.1	On the evaluation of the SFR-results, a pass or fail is given in the evaluation report.
	2m	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.	Evaluation of the functionalities to destroy keys and data, and of the security architecture: FCS_CKM.6 AGD_OPE.1 ADV_ARC.1	On the evaluation of the SFR/SAR-results, a pass or fail is given in the evaluation report.
NOTE: The summary analysis given in the OND [4] requirements catalogue did not include an analysis against the cited SARs.				

Table B.2: Essential Cybersecurity requirements relating to Vulnerability handling requirements of products with digital elements

Id	Text from CRA - Annex I	Test process	Determination
Manufacturers of products with digital elements shall			
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.	Evaluation of the provided vulnerability processing covering the reception, examination, the assignment of its nature and risk, and the assignment of the affected component using an SBOM.	Based on the coverage of provided vulnerability process documentation covering the aspect in question, a pass or fail of the CRA SR is given in the evaluation report.
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.**	Evaluation of the mitigation means in dependency of the before made nature and risk assignment. The description should cover the aspects. Evaluation of the procedure for the provision of security updates.	Based on the coverage of provided vulnerability process documentation covering the aspect in question, a pass or fail of the CRA SR is given in the evaluation report.
3	Apply effective and regular tests and reviews of the security of the product with digital elements.	Evaluation of the development security testing process documentation.	Based on the coverage of provided vulnerability process documentation covering the aspect in question, a pass or fail of the CRA SR is given in the evaluation report.
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.**	Evaluation of the provided vulnerability processing, including now the policy for coordinated public disclosure procedures after provision of mitigations to the users.	Based on the coverage of provided vulnerability process documentation covering the aspect in question, a pass or fail of the CRA SR is given in the evaluation report.
5	Put in place and enforce a policy on coordinated vulnerability disclosure.	Evaluation of the provided vulnerability processing, including now the policy for disclosure.	Based on the coverage of provided vulnerability process documentation covering the aspect in question, a pass or fail of the CRA SR is given in the evaluation report.

Id	Text from CRA - Annex I	Test process	Determination
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.	Evaluation of the provided vulnerability processing, including now the policy for disclosure of the vulnerability to affected third party component suppliers based on the SBOM.	Based on the coverage of provided vulnerability process documentation covering the aspect in question, a pass or fail of the CRA SR is given in the evaluation report.
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.	Evaluation of the security update provision facility, and, depending on the administration of the TOE, whether an automated download is configurable.	Based on the coverage of provided vulnerability process documentation covering the aspect in question, a pass or fail of the CRA SR is given in the evaluation report.
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.	Evaluation of the provided vulnerability processing, including now the policy for disclosure of the vulnerability and the related communication.	Based on the coverage of provided vulnerability process documentation covering the aspect in question, a pass or fail of the CRA SR is given in the evaluation report.
NOTE: For vulnerability reporting in general the provisions of the ALC_FLR - Flaw Remediation, defined in [i.9] apply, in particular ALC_FLR.2, Evaluation of flaw remediation wherein the evaluator assesses the overall flaw remediation process of the developer. This is addressed more fully in the derived EUCC PP of ETSI TS 103 996 [i.4].			

History

Document history		
V1.1.1	September 2025	Publication