ETSI TS 103 963 V1.1.1 (2023-12)

CYBER;
Optical Network and Device Security;
Security provisions in transport network devices

Reference
DTS/CYBER-0093

Keywords
cybersecurity, optical network device,
security requirements

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 Web server (https://ipr.etsi.org/).

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™** and **LTE™** 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.

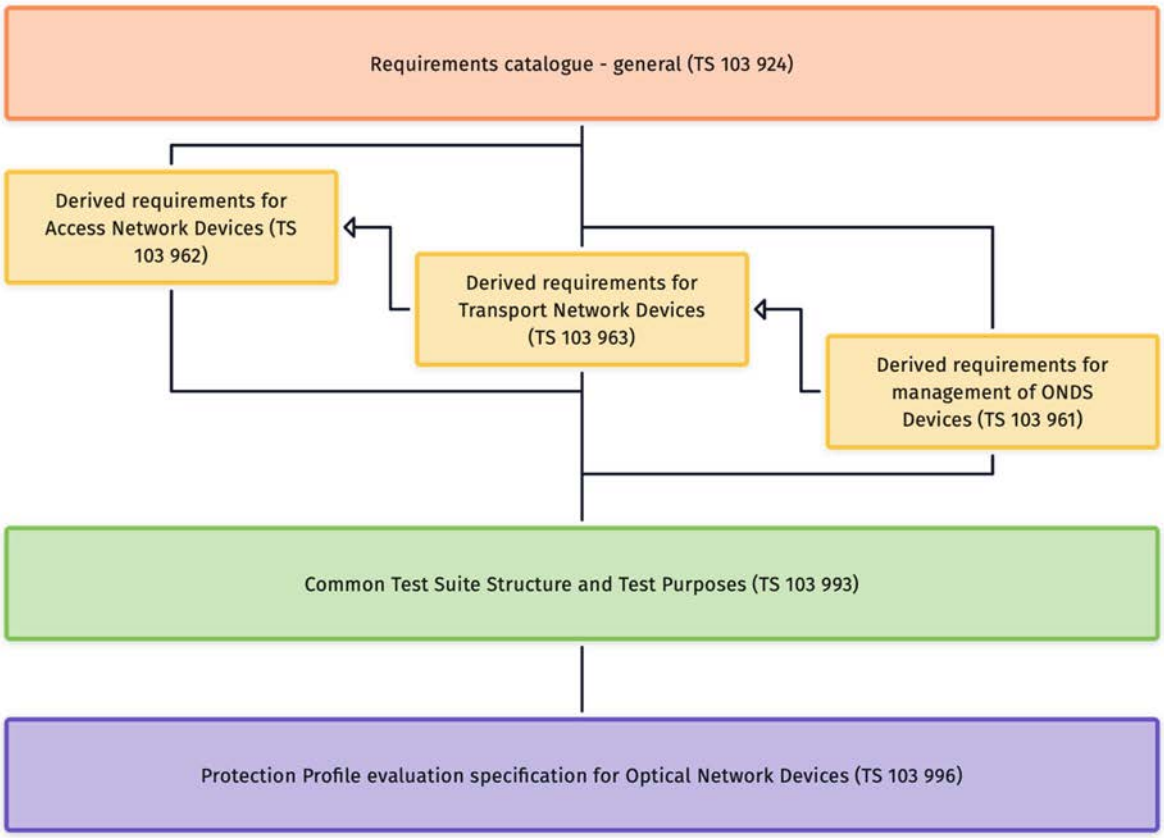

Figure 1: Document structure for Optical Network Device Security

Each of ETSI TS 103 962 [6], ETSI TS 103 963 (the present document) and ETSI TS 103 961 [2] expand upon the requirements identified in the common catalogue of ETSI TS 103 924 [1]. In the definition of detailed provisions ETSI TS 103 962 [6] acts as the master document with each of the present document and ETSI TS 103 961 [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 [i.6], and from that is derived a specification of the evaluation assessments to be applied, this document, ETSI TS 103 996 [i.7], is given in the form of a partial protection profile.

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 provides the baseline requirements specific to optical transport network devices.

The present document extends the provisions identified in the Catalogue of Requirements for Optical Network and Device Security from ETSI TS 103 924 [1] (see also Annex B of the present document) addressing the optical network entities to optical core/backbone and optical intra-core interfaces. The present document gathers the requirements in the form an Implementation Conformance Statement in Annex A.

2 References

2.1 Normative references

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

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

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 103 924: "Optical Network and Device Security; Catalogue of Requirements".

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

[3] FIPS 140-2: "Security Requirements for Cryptographic Modules".

[4] NIST SP 800-90B: "Recommendation for the Entropy Sources Used for Random Bit Generation".

[5] 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: An update to the work item above is in development but the latest draft is publicly available.

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

[7] ETSI EN 303 645: "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

[8] ETSI TS 103 848 (V1.1.1): "Cyber Security for Home Gateways; Security Requirements as vertical from Consumer Internet of Things".

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 are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 103 486: "CYBER; Identity Management and Discovery for IoT".

NOTE The work item above is in development but the latest draft is publicly available.

[i.2] NIST SP 800-160 Vol.1 Rev.1: "Developing Cyber Resilient Systems: A Systems Security Engineering Approach".

[i.3] Recommendation ITU-T G.709: "Interfaces for the optical transport network".

[i.4] INCITS 359-2012: "Information Technology -- Role-Based Access Control" (May 29, 2012).

[i.5] NIST SP 800-162: "Guide to Attribute Based Access Control (ABAC); Definition and Considerations".

[i.6] ETSI TS 103 993: "Cyber Security (CYBER); ONDS; Test Suite Structure and Test Purposes".

[i.7] ETSI TS 103 996: "Cyber Security (CYBER); ONDS; Protection profile - Test cases".

[i.8] ETSI TR 103 838: "Cyber Security; Guide to Coordinated Vulnerability Disclosure".

[i.9] Proposal for a Regulation on cybersecurity requirements for products with digital elements - Cyber resilience (CRA).

[i.10] US Cybersecurity Framework.

[i.11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

canonical identifier: structured identifier that is globally unique

root identity: canonical identifier of the device that is attested to in the root identity certificate of the device

3.2 Symbols

Void

3.3 Abbreviations

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

ABAC	Attribute Based Access Control
CIA	Confidentiality Integrity Availability
C-MAC	Cipher-Message Authentication Code
CRA	Cyber Resilience Act
CRC	Cyclic Redundancy Check
CTR	CounTeR (mode)
DPIA	Data Protection Impact Assessment
FEC	Forward Error Correction
GCM	Gallios Counter Mode
GDPR	General Data Protection Regulation

GEM	GPON Encapsulation Method
GPON	Gigabit Passive Optical Network
ICS	Implementation Conformance Statement
ICV	Integrity Check Value
IP	Internet Protocol
MAC	Message Authentication Code
NMS	Network Management System
OAN	Optical Access Network
OLT	Optical Line Termination
ON	Optical Network
ONDS	Optical Network Device Security
ONDS-M	ONDS-Manager
ONT	Optical Network Termination
ONU	Optical Network Unit
OPU	Optical Payload Unit
OTH	Optical Transport Header
OTN	Optical Transport Network
OTU	Optical Transport Unit
PCB	Printed Circuit Board
PON	Passive Optical Network
RBAC	Role Based Access Control
RoT	Root of Trust
RtS	Root of trust for Storage
SA	Security Association
TVP	Time Variant Parameter
XOR	eXlusive OR (binary operation)

4 Overview of security of functions for OTN

4.1 OTN device functional model

The general provisions stated in ETSI TS 103 924 [1] and from ETSI TS 103 962 [6] apply to ON devices operating within the transport network with the additional specializations given in the present document.

NOTE: Provisions extended from [1] that apply solely to access devices are described in ETSI TS 103 962 [6].

Clause 4.1 of ETSI TS 103 962 [6] applies with the following clarifications and extensions.

The OTN devices defined in the present document consists of multiple ON devices and their connections.

This OTN is used to carry client signals. Payloads are encoded into an Optical Data Unit (ODU) whose overhead enables network services to operate (e.g. path monitoring and tandem connection monitoring) and then encoded for transport into Optical Transport Units (OTU). The OTN shall also support the management and control functions in each ON transport device as described in ETSI TS 103 961 [2].

4.2 Trust architecture in ON transport device

Clause 4.2 of ETSI TS 103 962 [6] applies with the following clarifications and extensions.

Where reference is made in ETSI TS 103 962 [6] to an Access device it shall be read as apply to an ON transport device for the present document.

5 Identification and authentication of OTN devices

The provisions of ETSI TS 103 962 [6] apply with the replacement of the term "access" with "transport". With respect to the role and application of random numbers a reference is made to the bibliography in which a number of articles and opinions on the use of software only random numbers are cited all of which suggest that such sources are inadequate for use in cryptographic operations.

6 Confidentiality and integrity protection of data transfer between OTN devices

6.1 General provisions - integrity

The provisions of ETSI TS 103 962 [6], clause 6.1 apply with the replacement of access device by transport device.

6.2 General provisions - confidentiality

The provisions of ETSI TS 103 962 [6], clause 6.2 apply with the replacement of access device by transport device and the following text applies.

All transmissions between OTN devices should be protected by a confidentiality security association. Where used the security association should identify:

1) The encryption algorithm.

2) The mode used for application of the algorithm (CounTeR mode (CTR), Galois Counter Mode (GCM), etc.) (see ETSI TS 102 165-2 [5]).

3) The end points.

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.

In addition, different service data transferred from the Client device, e.g. OLT, towards the network shall be isolated from each other.

EXAMPLE: Isolation of service data is a native function of the OTN protocols defined in Recommendation ITU-T G.709 [i.3], wherein different service data is encoded into different ODU, then encoded or mapped into OTU.

7 Secure data storage on OTN devices

7.1 General provisions

For protection of management and configuration data the provisions of ETSI TS 103 961 [2] and of ETSI TS 103 962 [6] apply

7.2 Access control in OTN devices

The provisions identified in ETSI TS 103 924 [1], ETSI TS 103 961 [2] and ETSI TS 103 962 [6] apply with the additional detailed provisions identified in the present document (see also Annex B).

Consistently with ETSI TS 102 165-2 [5] the Optical transport network access control model defines Permission (allow, do not allow (alternatively permit, do not permit)) as a function of "Subject", "Action", "Object" extended by "Context", where each of "Subject", "Action" and "Object" and "Context" are as defined in the present document and in ETSI TS 103 961 [2] and where Permission is evaluated using the set model identified in ETSI TS 102 165-2 [5] and copied below, with the rule that permission is granted only when all conditions in the policy pass. Context in the present document and for the purposes of this clause includes attributes such as subject-location, time of the access attempt:

- $s \in S$
- $a \in A$
- $o \in O$
- $c \in C$
- $P\ \exists!\{S \cup A \cup O \cup C\}\ for\ any\ s, a, o, c$

The set of "Subject" may include the following (each list element is a member, s, of the set S (the list is indicative)):

- OA-Management entity (defined in ETSI TS 103 961 [2]) (as a role);
- Client-side management entity (as a role);
- Device-administrator (as a role); and
- Security credentials manager (as a role).

The set of "Object" may include the following:

- Configuration data.
- Cryptographic keys.

The context parameter set in any rule may include the following (the list is indicative):

- Local access.
- Remote access.
- Permitted access time.

Each protected Object in the OTN device shall be protected by a policy that shall be evaluated on each access attempt. The policy shall consist of 1 or more rules each of which shall be evaluated in turn. Every denied access attempt shall be recorded where the record 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. In addition if an object has multiple access control errors (i.e. multiple access attempts are denied) the OTN device, in collaboration with the ONDS-M, shall set a reporting threshold for making an exception report.

NOTE 1: It is assumed that all functional and data assets of the OTN Device are protected.

EXAMPLE: If an arbitrary subject attempts to access an object more than *n* times in time *t* (the reporting threshold) an exception report is made.

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. If an exception is raised it shall include the details of the rule that failed.

The default access control condition for all objects shall be "do not allow"/"do not permit".

NOTE 2: In the present document a rule is identified as any single calculation of the P ∃!{S∪A∪O∪C} formula, and a policy is any combination of rules.

NOTE 3: The access control model described is similar to that of Attribute Based Access Control (ABAC) [i.5] but if restricted to subjects that only represent a role, and where the context is null, the model described is similar to that of Role Based Access Control (RBAC) [i.4].

7.3 Access Control rules for OTN devices

The following rules shall be implemented in OTN devices.

NOTE 1: Access control rules are atomic and identify only one condition per rule.

Rule CFG-AC Descriptive format: Only a device administrator shall be allowed to update, or delete, an entry in the configuration data object.

- P ∃!{S∪A∪O∪C} shall be true only when Object (o) = Configuration data, Action (a) = Update XOR Delete, Subject (s) = Device-administrator, Context (c) = Null

Rule CK-AC descriptive format: Private cryptographic keys shall only be accessible by the relevant algorithm and shall not be directly retrievable from the device.

- (1) P ∃!{S∪A∪O∪C} shall be true only when Object (o) = Private cryptographic key, Action (a) = Read, Subject (s) = Algorithm, Context (c) = Null
- (2) P ∃!{S∪A∪O∪C} shall be true only when Object (o) = Private cryptographic key, Action (a) = Copy XOR Move, Subject (s) = Algorithm, Context (c) = Null

NOTE 2: It may be necessary to move the key from a permanent store to be used in volatile memory as part of the cryptographic processing in which case the rules above still apply as control is retained by the algorithm.

NOTE 3: The principle of least persistence applies whenever volatile memory is used whereby the content of such memory is erased after use.

Rule DEV-AC descriptive format: Only a device with pre-configured attributes can connect to the OTN device.

- P ∃!{S∪A∪O∪C} shall be true only when Object (o) = Network, Action (a) = Connect, Subject (s) = Device with pre-configured attributes, Context (c) = Null

EXAMPLE 1: An OTN device may reject all management terminal expect the one matching the IP or MAC address pre-configured on the OTN device.

Rule PAC-AC descriptive format: Packets that match certain pre-configured attributes shall be dropped.

- P ∃!{S∪A∪O∪C} shall be true only when Object (o) = Network packet with pre-configured attributes, Action (a) = Drop, Subject (s) = Network stack, Context (c) = Null

EXAMPLE 2: An OTN device may reject all network packet matching the IP or MAC address pre-configured block list on the OTN device.

7.4 Access control policy in OTN devices

An access control policy combines rules into an overall access control condition.

As above the overall policy should be defined in such a way that all rules of a policy have to pass in order to permit access.

A policy shall only set access control permission to True where all rules of any policy pass (i.e. the only combination of rules is by logical AND.

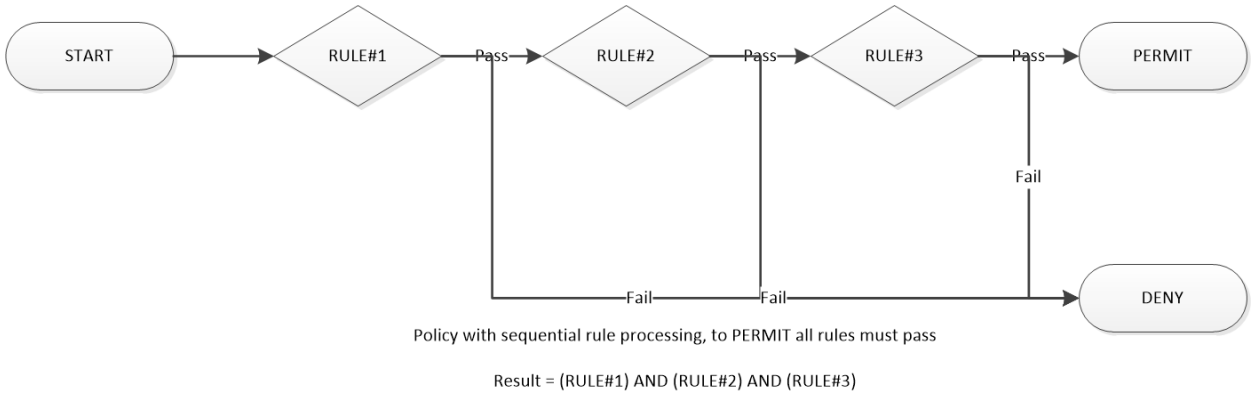

Figure 2: Access control combining rules (attribute settings) where all rules have to pass

Annex A (normative): ICS Pro forma

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document may freely reproduce the ICS pro forma in this annex so that it can be used for its intended purposes and may further publish the completed ICS.

Table A.1 of the present document is based on that found in ETSI EN 303 645 by the addition of the requirements specified in the present document for the OTN Devices.

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document can freely reproduce the pro forma in the present annex so that it can be used for its intended purposes and can further publish the completed annex including table A.1.

Table A.1 can provide a mechanism for the user of the present document (who is expected to be an entity involved in the development or manufacturing of an OTN Device) to give information about the implementation of the provisions within the present document.

The reference column gives reference to the provisions in the present document.

The status column indicates the status of a provision. The following notations are used:

M the provision is a mandatory requirement

R the provision is a recommendation

M C the provision is a mandatory requirement and conditional

R C the provision is a recommendation and conditional

NOTE: Where the conditional notation is used, this is conditional on the text of the provision. The conditions are provided at the bottom of the table with references provided for the relevant provisions to help with clarity.

The support column can be filled in by the user of the present document. The following notations are used:

Y supported by the implementation

N not supported by the implementation

N/A the provision is not applicable (allowed only if a provision is conditional as indicated in the status column and if it has been determined that the condition does not apply for the product in question)

The detail column can be filled in by the user of the present document:

- If a provision is supported by the implementation, the entry in the detail column is to contain information on the measures that have been implemented to achieve support.
- If a provision is not supported by the implementation, the entry in the detail column is to contain information on the reasons why implementation is not possible or not appropriate.
- If a provision is not applicable, the entry in the detail column is to contain the rationale for this determination.

Table A.1: Implementation of provisions for OTN Device security

Item	Requirement	Status	Support	Details
Req-1	ON systems shall be designed to be secure by default and to support the functionality required by the CIA paradigm.	M		
Req-2	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 network.	M		

Item	Requirement	Status	Support	Details
Req-3	Any link enabled during, and post-initialization, shall support periodic re-establishment of the security association.	M		
Req-4	The principles of least privilege and least persistence shall be applied.	M		
Req-5	In accordance with the least persistence principle security associations shall not be maintained for longer than required.	M		
Req-6	If any software verification fails that software and any supporting elements shall not participate in any security association.	M		
Req-7	All ON entities shall be able to report the form of CIA protections that are available and operational to authorized entities.	M		
Req-9	An OTN device's execution environment shall have 1 (one) initial root of trust	M		
Req-10	The execution environment shall have at least one executable code block.	M		
Req-11	The OTN Device shall have a root of trust used for initialization to enable secure boot capabilities.	M		
Req-12	The OTN 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-13	The manufacturer of the OTN Device shall attest to the provision of the root of trust by reference to the method applied.	M		
Req-14	The presence of the hardware root of trust shall be asserted by a platform specific attribute certificate.	M		
Req-15	All cryptographic modules shall be designed to be crypto-agile.	M		
Req-16	The specific cryptographic algorithms for each security association shall be defined by the security policy.	M		
Req-17	Cryptographic algorithms should be sufficient to inhibit known cryptanalysis attacks and mechanisms.	R		
Req-18	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		
Req-19	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		
Req-20	All ON devices shall be identified with a canonical/root identity and, optionally, additional semantic identifiers identifying their functional nature.	M		
Req-21	Where provided, the semantic identifier shall be used to indicate the functional nature of the entity.	M C		
Req-22	The attestation of function should be verifiable by reference to a 3rd party.	R		
Req-23	The authentication process shall verify the ON entity's identity (e.g. a globally unique device address) to a shared key assignment.	M		
Req-24	The to be authenticated identity shall be an attribute of the authentication protocol.	M		
Req-25	The identity shall always be authenticated on first presentation and periodically thereafter.	M		
Req-26	In order to be consistent with the principle of least persistence an authenticated session shall expire after a set time.	M		
Req-27	The length of an authentication session shall be set by the Authentication-Session-Time-Limit variable.	M		
Req-28	The Authentication-Session-Time-Limit variable shall be established for each security association.	M		

Item	Requirement	Status	Support	Details
Req-29	A device shall be identified in order to be admitted to the operator's trust domain.	M		
Req-30	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		
Req-31	Any identifier presented by the device shall be authenticated by the receiving device.	M		
Req-32	A key shall be associated to an attribute or identifier of the OTN Device.	M		
Req-33	The binding of key to the attribute or identifier shall be maintained for each security association.	M		
Req-34	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		
Req-35	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		
Req-36	The MAC approach to authentication as outlined in ETSI TS 102 165-2 shall apply.	M		
Req-37	Random challenges used in any MAC based authentication shall be generated using a true source of randomness.	M		
Req-38	Software only functions shall not be used to generate random challenges.	M		
Req-39	A challenge-response method should be used at initialization and for key establishment, key refresh, events.	R		
Req-40	Only cryptographically relevant challenge response schemes shall be used.	M		
Req-41	The challenge response approach to authentication as outlined in ETSI TS 102 165-2 shall apply.	M		
Req-42	Random challenges used in any challenge-response protocol shall be generated using a true source of randomness.	M		
Req-43	The self-attestation shall be provided in the form of a digital signature and include a signed public key.	M C		
Req-44	In order to perform self-attestation of identity the OTN device should be able to securely generate cryptographic keys associated with identifiers, and to securely store the private cryptographic material.	M C		
Req-45	The OTN 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		
Req-46	The OTN device shall have a root of trust for storage to store private cryptographic material (private key).	M		
Req-47	In accordance with ETSI TS 103 486 the identity (canonical) and identifying attributes of a device should be attested to by an appropriate independent 3rd party.	R		
Req-48	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		
Req-49	A device should only be able to perform a self-attestation of its capability at initialization.	R C		
Req-50	The self-attestation shall be provided in the form of a digital signature and include a self-signed public key.	M C		

Item	Requirement	Status	Support	Details
Req-51	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		
Req-52	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		
Req-53	All exchanged discrete messages shall have their integrity verified on reception at the device if the presence of the integrity check value clearly indicated.	M		
Req-54	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		
Req-55	Any message that fails the integrity check shall be discarded and an error reported.	M		
Req-56	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		
Req-57	All transmissions between OTN devices should be protected by a confidentiality security association	R		
Req-58	Where used the security association should identify: The encryption algorithm; The mode used for application of the algorithm; the end points.	R C		
Req-59	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		
Req-60	Every OTN device shall have a root of trust for storage (RtS).	M		
Req-61	All data in OTN devices shall be made available to authorized entities using the principle of least privilege.	M		
Req-62	The access control mechanism shall follow the policy model outlined in ETSI TS 102 165-2.	M		
Req-63	Each protected Object in the OTN device shall be protected by an access control policy.	M		
Req-64	The access control policy shall be evaluated on each access attempt.	M		
Req-65	The policy shall consist of 1 or more rules each of which shall be evaluated in turn.	M		
Req-66	Every denied access attempt shall be recorded.	M		
Req-67	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		
Req-68	If an object has multiple access control errors the OTN device, in collaboration with the ONDS-M, shall set a reporting threshold for making an exception report.	M		
Req-69	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		
Req-70	If an exception is raised it shall include the details of the rule that failed.	M		
Req-71	The default access control condition for all objects shall be "do not allow"/"do not permit".	M		
Req-72	The following rules shall be implemented in OAN devices: CFG-AC; CK-AC; DEV-AC; PAC-AC.	M		

Item	Requirement	Status	Support	Details
Req-73	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		
Req-74	A policy shall only set access control permission to True where all rules of any policy pass.	M		

Annex B (normative): Mapping to common requirements from ETSI TS 103 924

NOTE 1: The present document extends the requirements from ETSI TS 103 924 [1], therefore this annex identifies where any extension can be found in the present document.

NOTE 2: The references from ETSI TS 103 924 [1] are suppressed in the following table.

Table B.1: Mapping to ETSI TS 103 924 [1]

Source in ETSI TS 103 924 [1]	M/O/C	Applicable text	Provision in the present document
Clause 4.5	O	*"With respect to confidentiality the user content of an optical transmission **should** not be available to an attacker even if the raw data is intercepted."*	The mechanisms to provide confidentiality of user content in transmission are defined in clause 6.2 of the present document.
Clause 4.5	O	*"Endpoints of each link **should** be uniquely identifiable, and **should** be able to verify their identity (i.e. their identity should be verifiable by a 3rd party)."*	The mechanisms to provide identification and authentication are given in clause 5 of the present document.
Clause 4.5	O	*"Data (content, control, signalling) that is essential to the management of the network **should** only be visible to authorized entities in the network."*	The mechanisms to provide access control are given in clause 7.2 of the present document.
Clause 5.1	M	*"Within the optical network, entities **shall** be able to be uniquely identified to each other element within a single trusted domain."*	The mechanisms to provide identification and authentication are given in clause 5 of the present document.
Clause 5.1	M	*"For each of Connection confidentiality and Connectionless confidentiality the confidentiality service **shall** be bound to the semantic and canonical identifier of the terminator of the service."*	The management of security associations is outlined with respect to ETSI TS 103 961 [2] in clauses 5, 6 and 7 of the present document.
Clause 5.2	M	*"The authentication **shall** verify the ON entity's identity to the shared key assignment and the to be authenticated identity **shall** be an attribute of the authentication protocol."*	The management of security associations is where authentication is bound to key assignment is outlined with respect to the use of MACs in clause 5 of the present document.
Clause 5.2	M	*"Any random challenges required in the authentication protocol **shall** be generated using a method as described in Annex C of FIPS 140-2 and using the model of non-determinism from NIST SP 800-90B."*	See clause 5 of the present document.
Clause 6.1	M	*"Confidentiality protection **shall** be applied, in the OTN, to the OPU prior to its encapsulation in an ODU (the header elements of the ODU are required for system control). In the OAN the protection **shall** be applied to the GPON Encapsulation Method (GEM) Frame using an identical mechanism (i.e. the base confidentiality protection mechanism is the same whether applied to an OPU or a GEM frame). Confidentiality protection **shall** be achieved by encryption of the OPU or GEM Frame using an appropriate algorithm using an appropriate mode."*	See clause 6.2 of the present document.
Clause 6.1	M	*"The CRC defined in Recommendation ITU-T G.975 and Recommendation ITU-T G.975.1 **shall** be applied to the encrypted payload (see also clause 7.2)."*	Not updated by the present document.
Clause 6.2.1	M	*"The keys **shall** be stored in a hardware based secure element acting as a Root of Trust (RoT). A key manager **shall** be instigated at the network core and **shall** distribute keys."*	See clause 6.

Source in ETSI TS 103 924 [1]	M/O/C	Applicable text	Provision in the present document
Clause 6.2.2	M	*"Each element **shall** be able to create an asymmetric key pair and have it certified within a designated trust domain. Each element **should** have the capability to import certificates, and act appropriately on revoked certificates (including marking their own certificates as revoked)."*	See clause 5 of the present document.
Clause 7.1	M	*"In order to give higher assurance of system reliability OTH defines the use of Forward Error Correcting (FEC) codes in Recommendation ITU-T G.975 calculated using a Reed-Solomon coding scheme across the payload columns. The FEC codes are not mandatory to implement in Recommendation ITU-T G.709 but **shall** be implemented for the purposes of the present document and **shall** apply after data encryption (as defined in clause 6) and any cryptographic data integrity protection (as defined in clause 7.3) have been applied (on transmission)."*	Not updated by the present document.
Clause 7.2	O	*"The risk analysis in Annex A suggests that malicious modification of data in transit is unlikely without significantly increasing either jitter or latency in the connection (see also Recommendation ITU-T X.800 where data integrity services are only considered as applicable at layer 3 and above). However management data is a special case and **should** be protected from malicious interference."*	Not updated by the present document.
Clause 7.2	M	*"The content of all management protocol units **shall** be protected using a keyed Message Authentication Code (MAC) process and thus **shall** be directly linked to the identification and authentication service relating to the identity of the management entity in any OTN or OAN device. Details of the MAC process and top level operation are described in clause 5.4.3 of ETSI TS 102 165-2. The C-MAC **should** use a key derived from the authentication process (see clause 5) and distinct from that used in the confidentiality service (see clause 6).*	See clause 6.1 of the present document.
Clause 7.3	O	*ONs **should** apply best practice. In particular any security data, e.g. keys, certificates, **should** be maintained in a hardware root of trust for storage.*	Not updated by the present document.
Clause 7.4	M	*As shown in Figure 2, an ONT or an ONU connects to an OLT. There is no message integrity checking mechanism defined in first-generation GPON network, see Recommendation ITU-T G.984.3, however for the purposes of the present document for the management message channel (PLOAM, OMCI) (see XGS-PON in Recommendation ITU-T G.9807.1) enhanced integrity protection **shall** be used using the mechanisms identified in the current clause."*	Not updated by the present document.

Source in ETSI TS 103 924 [1]	M/O/C	Applicable text	Provision in the present document
Clause 8.1	O	*"The capabilities defined in Recommendation ITU-T G.987 series, Recommendation ITU-T G.989 series, and Recommendation ITU-T G.9807.1 as applied to each of XG-PON, NG-PON2, and XGS-PON systems apply and **should** be implemented as appropriate to the specific technology. An extension defined in Supplement 51 to Recommendations ITU-T G-series further develops the specifications and **should** be applied as appropriate to the specific technology.*	Not updated by the present document.
Annex A	O	*ETSI TR 103 305-1 identifies a set of 18 critical security controls as follows and their application in ONs. Where a control is identified as not applicable this is only with respect to the technology as used in ONs, and should be not be taken as implying that the control is not valid for the organization deploying ONs where a different answer is almost inevitable."*	Not updated by the present document.
Clause B.2	O	*"With respect to services and service placement the reference model of Figure B.1 identifies a number of groupings (as planes) of security functions as follows. For each plane of functions there **should** be a Root of Trust in the hardware in which the function resides."*	Not updated by the present document.
Annex C	O	*"Thus, an SA between 2 ON/OTN entities can exist for each of the CIA attributes, and be managed by a distinct Key-management policy. The Key management policy **should** include key-refresh policies (i.e. when the key should be renewed)."*	Not updated by the present document.

Annex C (normative): Environmental, deployment, and development constraints

In implementing and deploying an OTN device a number of requirements apply to the environment. These apply either to the development environment or to the deployment environment and are outlined here. These apply in addition to the specific device requirements given in the main body of the present document but are not part of the ICS as they do not directly impact the device.

NOTE: Many of the requirements in this annex cannot be tested by automated test scripts to give a definitive pass or fail judgement but can only be tested by direct inspection of the installation or by 3rd party assessment of the development process.

Table C.1: Requirements placed on the deployment of an OTN device

Reference	Requirement	Liable party
R-ENV-1:	The OTN shall be installed in such a manner that any interference with the OTN device-housing is detected and notified to the management authority.	Installation authority
R-ENV-1a:	If the device is in any operational state and Requirment-ENV-1 is satisfied the OTN should move a safe and default secure state (see note 1).	Operator policy
R-DPLY-1:	The device shall not contain any unnecessary physical interface on the enclosure and on its PCBs (see note 2).	Manufacturer
R-DPLY-2:	The debugging functions in software which can be used for troubleshooting shall not be activated during normal operation of the network product (see note 2).	Manufacturer
R-ENV-2:	The product installation shall protect the OTN device by ensuring that the device operates within its operational limits (e.g. temperature).	Installation authority
R-ENV-3:	The deployment environment should be able to detect smoke and fire to assist in maintaining device availability.	Installation authority
R-ENV-4:	Environmental monitoring should be available even if external power sources are unavailable (see note 3).	Installation authority
R-ENV-5:	If smoke or fire is detected an alarm should be sent to the system NMS.	Installation authority
NOTE 1: The details of what a safe and default secure state are, are for further study. NOTE 2: As indicated in ETSI EN 303 645 [7] non-operational elements should be removed prior to deployment, including any interfaces not required for operation, or software used for debug and similar operations. NOTE 3: Local regulations for device installation may apply.		

In addition to the requirements the development and maintenance of the OTN device should follow best practices, including addressing the requirements in ETSI EN 303 645 [7], in ETSI TS 103 848 [8], and the following.

Table C.2: Requirements placed on the development of an OTN device

Reference	Requirement	Liable party
R-DEV-01	Devices shall be developed in such a manner that only essential functions and network ports for the operation and maintenance of the device are provided (this is in addition to implementing the least privilege model identified in the main body of the present document).	Development authority (see note 1)
R-DEV-02	Devices shall be able to detect potential adversarial attack.	See note 2
R-DEV-03	If adversarial attack is suspected it shall be quarantined and reported to the security management entity.	See note 3
R-DEV-04	The manufacturer shall support a vulnerability disclosure scheme (see ETSI TR 103 838 [i.8]).	See note 4
R-DEV-05	Devices shall validate the source and integrity when updating system software.	Development authority
R-DEV-06	Devices shall be developed with defensive programming method to enhance the security of the software.	Development authority
NOTE 1: This is consistent with the least functionality principle of NIST SP 800-160 Vol.1 Rev.1 [i.2]. NOTE 2: Attack modelling should be shared across industry in order to co-operatively minimize the attack surface open to adversaries (see also vulnerability disclosure). NOTE 3: If the development authority implements the principles of least persistence, least privilege and least sharing as outlined in NIST SP 800-160 Vol.1 Rev.1 [i.2] any likelihood of exploit by an adversarial attack can be minimized. NOTE 4: Individual devices may support the vulnerability disclosure scheme through the reporting of exceptions to a reporting entity and by enabling updates of software.		

In addition the developer should take steps to maximize device security during the development cycle.

EXAMPLE: Where open source software is used the last stable release should be used, when compiling software the developer should use options in the compiler to minimize security risks.

Further requirements in this class are identified below for each of security auditing and logging, vulnerability reporting (in addition to the general requirements in ETSI TR 103 838 [i.8]).

Table C.3: Requirements for logging in support of security audit

Reference	Requirement	Liable party
R-LOG-01	Security events shall be logged together with a unique system reference (e.g. host name, IP or MAC address, userID or username) and the exact time the incident occurred.	
R-LOG-02	For each security event, the log entry shall include user name and/or timestamp and/or performed action and/or result and/or length of session and/or values exceeded and/or value reached.	
R-LOG-03	Any configuration change and setting shall be logged.	
R-LOG-04	Any attempt to update the device shall be part of the audit.	
R-LOG-05	No plain-text sensitive data or personal data shall be part of audit records.	
R-LOG-06	Devices shall be able to transmit the generated audit data to an external IT entity using a trusted channel.	
R-LOG-07	The security event log shall be access controlled so only privileged users have access to the log files.	

Table C.4: Requirements for vulnerability management and reporting

Reference	Requirement	Liable party
R-VLN-01	The manufacturer shall 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, severity of vulnerabilities and sufficient information to allow users to install the fix.	
R-VLN-02	The manufacturer shall allow customers to make vulnerability reports.	
R-VLN-03	The manufacturer shall not knowingly make available software with an exploitable vulnerability (see note 1).	
R-VLN-04	The manufacturer shall maintain software over a defined lifetime span that is at least equal to the minimum level required in any applicable legislation (see note 2).	
NOTE 1: If an exploit is discovered and a patch is available then this requirement is satisfied. NOTE 2: The support period for software should be clearly stated in the documentation related to the software.		

Annex D (informative): Requirements for placing OTN device on the market

Within the EU context an OTN device is a device containing digital elements and therefore the Cyber Resilience Act (CRA) [i.9] applies. For the US market context the provisions of the Cybersecurity Framework [i.10] apply.

Where any user data is gathered and maintained on the OTN device the scope of use of such data is subject to the constraints of the General Data Protection Regulation (GDPR) [i.11]. In such cases the rationale for holding such data on the device should be clearly defined and any necessary consent for use of such data recorded.

NOTE: An OTN device should, by default, not contain any user identifying data but this should be confirmed by in stage 1 of a Data Privacy Impact Assessment (DPIA).

Annex E (informative): Bibliography

E.1 Software random number generation

- Nadia Heninger, Zakir Durumeric, Eric Wustrow, J. Alex Halderman: "Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices".
- Aaron Kraus: "Why Random Numbers are Impossible in Software".

E.2 Regulatory instruments for placement on the EU market

- Cybersecurity Act (CSA), 2019.
- Digital Services Act (DSA), 11/2022.
- Critical Entity Resilience Directive (CER), 11/2022.
- Network and Information Security Directive 2 (NIS 2), 12/2022.
- Digital Operational Resilience Act (DORA), 01/2023.
- Machinery Regulation (MR), 05/2023.
- Radio Equipment Directive (RED), 02/2022.
- AIAct, Trilogue started 06/2023.
- Data Act, Trilogue ends maybe in 2023?
- e-Privacy Regulation (ePVO), Trilogue in 2023?
- Data Governance Act (DGA), entered into force on 23 June 2022, following a grace period of 15 months, applicable from 24 September 2023.

E.3 Other documents of interest

- ISO/IEC 9646-7: "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 7: Implementation Conformance Statements".
- Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".
- ISO 27002: "Information security, cybersecurity and privacy protection - Information security controls".

History

Document history		
V1.1.1	December 2023	Publication