ETSI TS 103 962 V1.1.1 (2023-12)

CYBER;
Optical Network and Device Security;
Security provisions in Optical Access Network Devices

Reference
DTS/CYBER-0092

Keywords
cybersecurity, optical access network,
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.

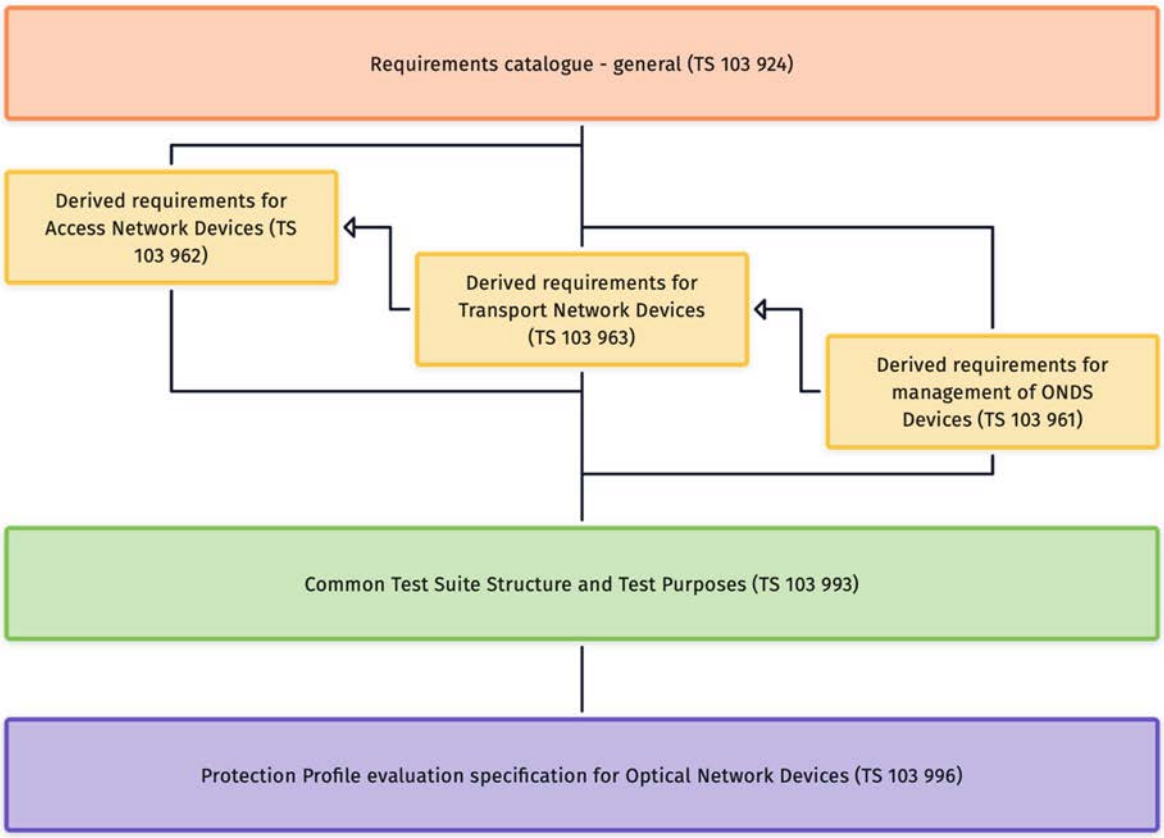

Figure 1: Document structure for Optical Network Device Security

Each of ETSI TS 103 962 (the present document), ETSI TS 103 963 [i.17] and ETSI TS 103 961 [3] expand upon the requirements identified in the common catalogue of ETSI TS 103 924 [1]. In the definition of detailed provisions. The present document acts as the master document with each of ETSI TS 103 963 [i.17] and ETSI TS 103 961 [3] 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.18] and from that is derived a specification of the evaluation assessments to be applied, this document, ETSI TS 103 996 [i.19], is given in the form of a partial protection profile.

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

1 Scope

The present document provides the baseline requirements specific to Optical Access Network (OAN) and devices which provides network access service to network service subscribers.

The present document extends the provisions identified in the Catalogue of Requirements for Optical Network (ON) and Device Security from ETSI TS 103 924 [1] addressing the security of Access Network (AN) and the Optical Line Terminal (OLT) as the core network equipment in Access Network.

The present document gathers the requirements in the form of an Implementation Conformance Statement in Annex A.

NOTE: A primacy distinction between OANs and OTNs (see ETSI TS 103 963 [i.17]) is in the lower layer protocols supported by the devices, OANs use GEM or GPON [2], [7] and [8] protocols to deliver client data, whereas OTNs device encode client data which come from an OLT device into an OTN frame transparently. However the optical transmission aspects are not addressed by the present document other than in the required security mechanisms needed to support them.

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] Recommendation ITU-T G.9804.1: "Higher speed passive optical networks - Requirements".

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

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

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

[6] Recommendation ITU-T G.9807.1: "10-Gigabit-capable symmetric passive optical network (XGS-PON)".

[7] Recommendation ITU-T G.987.3: "10-Gigabit-capable passive optical networks (XG-PON): Transmission convergence (TC) layer specification".

[8] 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.

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

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

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] Global Platform Security Task Force: "Root of Trust Definitions and Requirements, Version 1.0.1".

[i.2] NIST SP 800-164: "Guidelines on Hardware-Rooted Security in Mobile Devices (Draft)".

[i.3] ETSI TR 103 838: "Cyber Security; Guide to Coordinated Vulnerability Disclosure".

[i.4] ETSI GR ETI 002: "Encrypted Traffic Integration (ETI); Requirements definition and analysis".

[i.5] NIST SP 800-160 Vol.1 Rev.1: " Engineering Trustworthy Secure Systems".

[i.6] ISO/IEC 27002 (2022): "Information security, cybersecurity and privacy protection - Information security controls".

[i.7] Recommendation ITU-T G.984.3: "Gigabit-capable passive optical networks (G-PON): Transmission convergence layer specification".

[i.8] ETSI EG 203 310: "CYBER; Quantum Computing Impact on security of ICT Systems; Recommendations on Business Continuity and Algorithm Selection".

[i.9] ETSI GR QSC 004: "Quantum-Safe Cryptography; Quantum-Safe threat assessment".

[i.10] ETSI TR 103 619: "CYBER; Migration strategies and recommendations to Quantum Safe schemes".

[i.11] ETSI TS 133 501: "5G; Security architecture and procedures for 5G System (3GPP TS 33.501)".

[i.12] Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[i.13] IEEE 1609.2™: "IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Application and Management Messages".

[i.14] Proposal for a Regulation on cybersecurity requirements for products with digital elements - Cyber resilience (CRA).

[i.15] US Cybersecurity Framework.

[i.16] 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).

[i.17] ETSI TS 103 963: "CYBER; Optical Network and Device Security; Security provisions in transport network devices".

[i.18] ETSI TS 103 993: "Cyber Security (CYBER); ONDS Test Suite Structure and Test Purposes".

[i.19] ETSI TS 103 996: "Cyber Security (CYBER); ONDS Protection profile - Test cases".

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

EXAMPLE: An IMSI is an example of a canonical identifier.

crypto-agile: able to utilize crypto-agility

crypto-agility: property that permits changing or upgrading cryptographic algorithms or parameters

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:

AAT	Attribute Authority Tree
AEAD	Authenticated Encryption with Associated Data
AES-GCM	Advanced Encryption Scheme - Galois Counter Mode
CIA	Confidentiality Integrity Availability
C-MAC	Cipher based Message Authentication Code
ECDSA	Elliptical Curve Digital Signature Algorithm
FTTB	Fibre To The Building
FTTCab	Fibre To The Cabinet
FTTH	Fibre To The Home
IMSI	International Mobile Subscriber Identity
MAC	Message Authentication Code
NT	Network Termination
OAN	Optical Access Network
OLT	Optical Line Termination
ON	Optical Network
ONDS-M	Optical Network Device Security Manage
ONT	Optical Network Termination
ONU	Optical Network Unit
OTN	Optical Transport Network
PCB	Printed Circuit Board
PON	Passive Optical Network
RtS	Root of trust for Storage
SNI	Service Node Interface
SNMP	Simple Network Management Protocol
TCG	Trusted Computing Group
TLS	Transport Layer Security
TPM	Trusted Platform Manager
UNI	User Network Interface
XGS	10-Gigabit-capable symmetric passive optical network

4 Overview of security of functions for optical access network devices

4.1 Optical access network device functional model

The general provisions stated in ETSI TS 103 924 [1] apply to Optical Network (ON) devices operating in the access network with the additional specializations given in the present document. The access network is defined as the set of access links sharing the same network-side interfaces and supported by an optical access transmission system (see Recommendation ITU-T G 9804.1 [2]). The Optical Access Network (OAN) may include a number of Optical Network Units (ONUs) connected to the same Optical Line Termination (OLT). The OAN architecture is indicated in Figure 2. An access device shall distinguish and separate the user and network domains in the device.

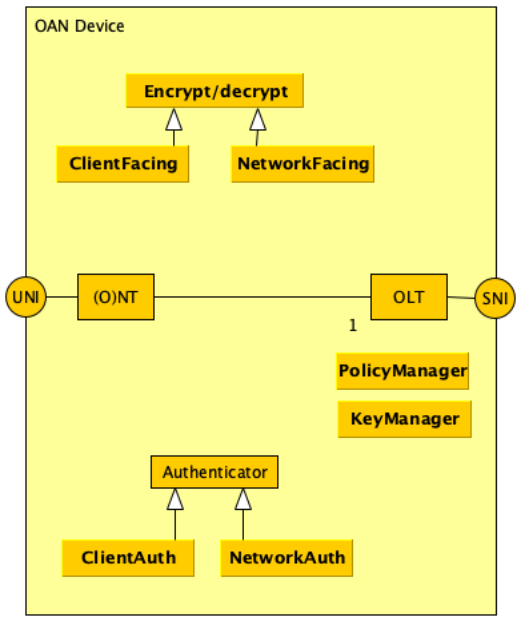

Figure 2: Optical Access Network device

The OAN and its associated devices consist of a single Optical Line Termination (OLT) facing the network side, one or more Optical Network Units (ONUs) and one or more Network Terminations (NTs) facing the client as shown in Figure 2.

NOTE: The ONU and the NT may be combined into a single unit and referred to as an Optical Network Termination (ONT).

When deployed the OAN device supports a suite of services the specific configuration of which is out of scope of the present document but examples of which are given in Annex E.

4.2 Trust architecture in Optical access network devices

As outlined in ETSI TS 103 924 [1] ON systems shall be designed to be secure by default and to support the functionality required by the CIA paradigm (Confidentiality, Integrity, Availability). 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. Any link enabled during, and post-initialization, shall support periodic re-establishment of the security association. The principles of least privilege and least persistence shall apply to all security associations. In accordance with the least persistence principle security associations shall not be maintained for longer than required. If any software verification fails (e.g. at power on test, at installation, at instantiation) that software and any supporting elements shall not participate in any security association.

NOTE 1: The term "for longer than required" is somewhat vague but is intended to convey that open-ended sessions with persistent security credentials are avoided, rather that a secured session with clear start and end conditions is adopted by default, where the end condition can include a timeout, i.e. the session is cleared after a set period.

All ON entities shall be able to report the form of CIA protections that are available and operational to authorized entities.

NOTE 2: In order to be consistent with the model of transparency and explicability identified in ETSI GR ETI 002 [i.4], in addition to the wider model of least privilege, all elements in the OAN-device and in the connected chain of devices that form any security association related to the devices and the services it supports it is expected that a management entity (local or remote) is able to interrogate the security status of any part of the ON including OAN devices.

4.3 Generalized functional model for an Optical access network device

An OAN device shall be integrated to the wider ON and telecommunications system of which it is a component and shall itself be decomposed into a set of functional elements with respect to security functionality as follows: an OAN device shall consist of at least 1 (one) execution environment which shall have 1 (one) initial root of trust (provisioned by the platform manufacturer and initialized during the manufacturing process and that is the first to be executed within the execution environment), and may have additional extended roots of trust (including those added by the operator). The execution environment shall have at least one executable code block and may have 0 (zero) or more associated data elements (including keys). In order to optimize separation of the client side, and network side, of the OAN device, there should be a discrete execution environment for each side and discrete roots of trust for each side.

NOTE 1: As illustrated in the deployment scenarios in Annex E the client side of an OAN device is able to support both single and multi-occupancy environments.

If an OAN device supports a multi-occupancy client environment (see Annex E) it shall provide confidentiality services at the client side to ensure physical (e.g. by managed allocation of virtual channels in the optical bearer) and cryptographic separation of distinct clients (i.e. if Client-A and Client-B are in a multi-occupancy termination of the OAN device it should not be feasible for Client-A to have any access to the traffic of Client-B).

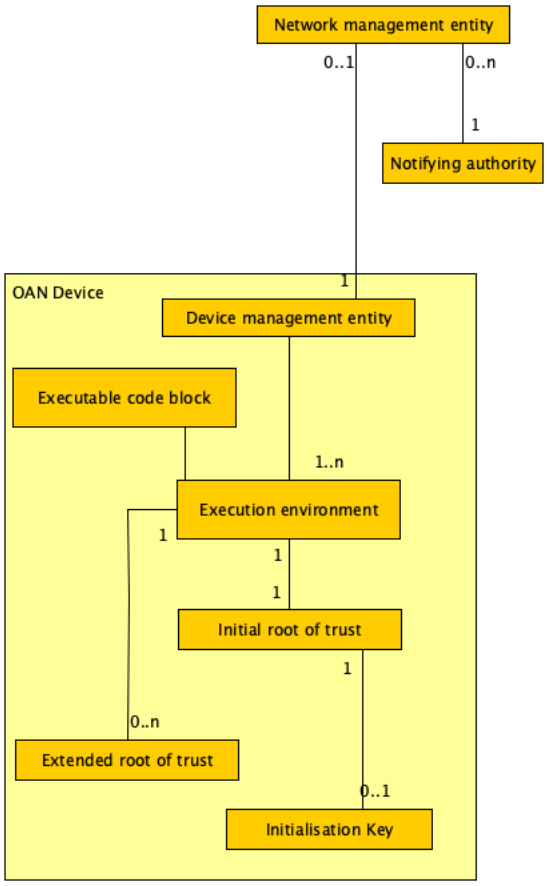

Figure 3: OAN Device functional architecture with respect to security and processing environments

As illustrated in Figure 3 the OAN Device shall have a root of trust used for initialization to enable secure boot capabilities. The root of trusts in the OAN Device shall be further decomposed as described below. 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.

The guidelines given in NIST SP 800-164 [i.2] shall be followed in order to provide the following local (device specific) trust services:

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

NOTE 2: The root of trust may be implemented in a number of ways including specific chipsets or by specific combinations of software and chipsets.

NOTE 3: It is not considered possible to verify the existence of a hardware root of trust by a protocol query.

The manufacturer of the OAN Device shall attest to the provision of the root of trust by reference to the method applied (e.g. a TCG conformant TPM) and shall publish that attestation in the technical specification of the OAN Device.

In addition, as identified in the definition for root of trust in NIST SP 800-164 [i.2], the presence of the hardware root of trust shall be asserted by a platform specific attribute certificate.

4.4 Guidance on cryptographic processes

All cryptographic modules shall be designed to be crypto-agile.

The specific cryptographic algorithms for each security association shall be defined by the security policy. Cryptographic algorithms should be sufficient to inhibit known cryptanalysis attacks and mechanisms (see also the impact of Quantum Computing on cryptography in ETSI EG 203 310 [i.8], ETSI GR QSC 004 [i.9] and ETSI TR 103 619 [i.10]).

NOTE: If during the period of use the installed cryptographic modules are found to be vulnerable (e.g. by new cryptanalysis or advances in computing or mathematics) the crypto-agility requirement allows the vulnerability to be managed by updating the cryptographic modules.

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.

4.5 Security error and misuse reporting

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.

EXAMPLE 1: Self-monitoring may use an Intrusion Detection System (IDS) to detect malicious activity.

EXAMPLE 2: If a device identifies a potential denial of service attack it reports it to the local device security manager process which should pass this message to a centralized authority in order to determine if the attack is local or distributed.

EXAMPLE 3: If an authentication failure is noted it should be locally reported, however if there are persistent failed attempts to authenticate this may indicate a pattern that can only be verified by reporting to a centralized authority.

5 Identification and authentication of Optical access network devices

5.1 Common provisions

The general provisions of the ON management standard (ETSI TS 103 961 [3]) apply wherein all devices shall be identified with a canonical/root identity and, optionally, additional semantic identifiers identifying their functional nature. The management entity, for the purposes of the present document, is referred to as the Optical Network Device Security Manager (ONDS-M). Where provided, the semantic identifier shall be used to indicate the functional nature of the entity and the attestation of function shall be verifiable by reference to a 3rd party. This is defined to be consistent with the Attribute Authority Tree (AAT) model described in ETSI TS 103 486 (see bibliography). As with the AAT model, it is not necessary to reveal all attributes of the device, rather only those attributes relevant to the current security association should be made visible in a manner consistent with the principle of least privilege (see also clause 7).

EXAMPLE: A device is delivered and uses its manufacturer defined serial number as its primary identity in which case the serial number is the canonical identifier, any attribute associated with the device, e.g. its functional class, is a semantic identifier and is bound to the canonical identifier which then acts as the "root" for the identity management of the device.

NOTE 1: The term "security association" is used in the widest sense to refer to the nature of the relationship between any instance of devices or products.

The authentication process shall verify the ON entity's identity (e.g. a globally unique device address) to a shared key assignment, and the to be authenticated identity shall be an attribute of the authentication protocol. The identity shall always be authenticated on first presentation and periodically thereafter. In order to be consistent with the principle of least persistence an authenticated session shall expire after a set time. The length of an authentication session shall be set by the Authentication-Session-Time-Limit variable that shall be established for each security association.

NOTE 2: The value assigned to the Authentication-Session-Time-Limit variable can be established by the ONDS-M or be explicit in the protocol used to establish the security association.

NOTE 3: If confidentiality protection uses an algorithm in Authenticated Encryption with Associated Data (AEAD mode), e.g. AES-GCM, the associated data may form an element for persistent authentication of data (over and above any use of an encryption key derived during the authentication phase).

NOTE 4: As above if an Encryption key is derived during authentication and is cryptographically linked to the authentication key then any exchange using such an encryption key is implicitly authenticated to the identity.

NOTE 5: The device unique address is out of scope of the present document but can include the device's card level network card address.

A device shall be identified in order to be admitted to the operator's trust domain. Within the trust domain the trust domain manager shall verify the capability of each device. Details of the overall management of the trust domain for secure devices in the ON are given in ETSI TS 103 961 [3] and devices in the scope of the present device shall comply to the requirements and provisions of ETSI TS 103 961 [3]. The considerations in Figure 4 apply in which an OAN device is attested by an authority to be an OAN device, and where access control, alongside the device class provides some restriction of the behaviour that can be exhibited by the OAN device.

NOTE 6: In any device there may be multiple discrete security trust associations to different elements in the operator's trust domain in which case the processes describe in the present document apply independently to each association.

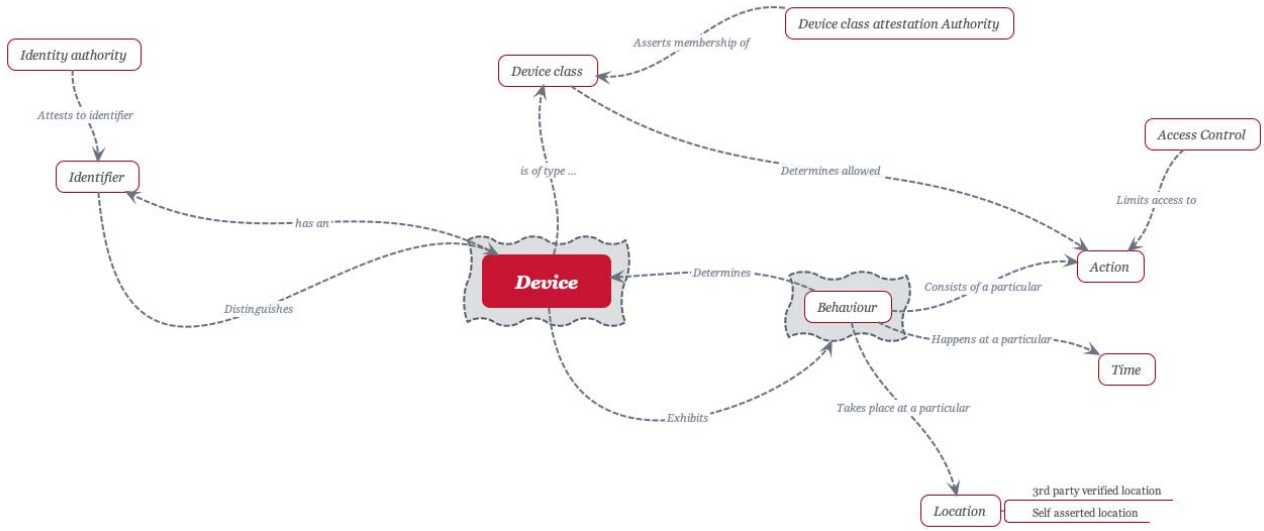

Figure 4: Management of device identifier and capability by attestation and access control

A device shall present an identifier to each of the client and the network side of the device. It should not be feasible to determine/infer the identifier presented to one side from knowledge of the identifier presented to the other side. As mandated above any identifier presented by the device shall be authenticated by the receiving device.

NOTE 7: The access control service shown in Figure 4 may include additional behavioural attributes to restrict the behaviour, and control of that behaviour (see also clause 7 of the present document).

NOTE 8: The form of managed identifier is defined in ETSI TS 103 961 [3].

NOTE 9: The permutation model described in ETSI TS 103 486 (see bibliography) therefore applies when identifying a device and its capability.

5.2 Identification and authentication

5.2.1 Symmetric keyed systems

5.2.1.1 Symmetric key distribution

The ONDS-M, defined in ETSI TS 103 961 [3], is responsible for ensuring that symmetric keys for each specific security association are made available at the device.

A key shall be associated to an attribute or identifier of the OAN Device. The binding of key to the attribute or identifier shall be maintained for each security association. In a fully symmetrically keyed system keys may be maintained in key-hierarchy with attribute keys derived from a single root key.

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 (appropriate to CIA purpose, e.g. AES for Encryption, SHA for integrity).

5.2.1.2 MAC based systems

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 (based on the mechanisms used in clause 6.2 of ETSI TS 133 501 [i.11]). If used the provisions in the present document apply.

The MAC approach to authentication as outlined in ETSI TS 102 165-2 [8] shall apply with the following restrictions/specializations.

Random challenges used in any MAC based authentication (for anti-replay and other protocol specific measures) shall be generated using a true source of randomness. The random challenge shall be generated from a source of appropriate entropy, in particular software only functions shall not be used to generate such challenges (see also clause 4.3 of the present document). As stated in ETSI TS 103 924 [1] (see annex B) any random challenges required in the authentication protocol shall be generated using a method as described in Annex C of FIPS 140-2 [9] and using the model of non-determinism from NIST SP 800-90B [10] or equivalent endorsed or mandated in specific markets.

NOTE: Where the OAN Device is an XGS-PON the mechanisms defined in Recommendation ITU-T G.9807.1 [6] apply using the ONU Management and Control Interface (OMCI) message exchange as per Annex C of Recommendation ITU-T G.987.3 [7].

5.2.1.3 Challenge response based systems

A challenge-response method should be used at initialization and for key establishment, key refresh, events. If used the provisions in the present document apply. Only cryptographically relevant challenge response schemes shall be used (i.e. the present document does not support challenge response based on non-cryptographic schemes (e.g. simple password comparisons)).

The challenge response approach to authentication as outlined in ETSI TS 102 165-2 [8] shall apply with the following restrictions/specializations.

Random challenges used in any challenge-response protocol shall be generated using a true source of randomness. In particular software only functions shall not be used to generate such challenges.

EXAMPLE 1: Encryption based approach: The challenger generates a random number N and encrypt it using the shared secret key and pre-defined algorithm and send this as the challenge. The recipient decrypts the challenge to recover N and sends the response N+1 encrypted with the shared secret key. (Challenge = N, expected response = N+1). The recipient is only able to send the correct expected response if both parties have access to the same shared secret.

EXAMPLE 2: Hash based approach: The challenger generates a Random Challenge (RC) and send the RC to the recipient. The recipient shall calculate the hash of the RC+shared-secret as Shared Response (SR) and send SR to the challenger. The challenger similarly calculates SR and verifies it is the same as that received. If the two values are the same it shows that both parties have access to the same shared secret.

NOTE 1: Where the OAN Device is an XGS-PON the mechanisms defined in Recommendation ITU-T G.9807.1 [6] apply using the X.802.1 methods as per Annex D of Recommendation ITU-T G.987.3 [7].

NOTE 2: It is recognized that it is not possible to verify using black box testing that the source of randomness is a hardware element and that an assertion by the manufacturer is required.

5.2.2 Asymmetric keyed systems (digital signature)

5.2.2.1 Self attestation of identity

A device should only be able to perform a self-attestation of its identity at initialization. The self-attestation shall be provided in the form of a digital signature and include a signed public key.

EXAMPLE: Digital self-attestation is done by creating a document, hashing it and encrypting the hash with the self-generated private key and distributing it with the public key. A recipient of the document determines the hash of the document and compares that hash with the decrypted hash (using the public key), if the hashes match the public key is provably associated to the private key and therefore the document (e.g. the identity) is self-attested.

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. Consequential requirements from supporting self-attestation of identity are:

- 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.
- The OAN device shall have a root of trust for storage to store private cryptographic material (private key). (See also clause 4.3 of the present document).

5.2.2.2 3rd party attestation of identity

The identity (canonical) and identifying attributes (see clauses 5.2.2.3 and 5.2.2.4) of a device should be attested to by an appropriate independent 3rd party.

NOTE: This is consistent with the Attribute Authority Tree framework described in ETSI TS 103 486 (see bibliography).

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.

EXAMPLE: An X.509 [i.12] identity certificate may be used to prove attestations of the canonical identifier of a device.

5.2.2.3 Self attestation of capability

A device should only be able to perform a self-attestation of its capability at initialization. The self-attestation shall be provided in the form of a digital signature and include a self-signed public key.

NOTE 1: In ETSI TS 103 486 each capability is identified as an attribute that is nominally independent of the root/canonical identity but is bound to it on creating an identified security association.

NOTE 2: In ETSI TS 103 486 each leaf attribute is also referred to as a semantic or contextual identifier.

5.2.2.4 3rd party attestation of capability

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.

NOTE: This is consistent with the Attribute Authority Tree framework described in ETSI TS 103 486 (see bibliography).

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.

EXAMPLE 1: An IEEE 1609.2 [i.13] certificate with appropriate labelling of the permissions field may be used to prove attestations of an attribute of a device.

EXAMPLE 2: An X.509 [i.12] attribute extension to an X.509 identity certificate may be used to prove attestations of an attribute of a device.

6 Confidentiality and integrity protection of data transfer between Optical access network devices

6.1 General provisions - integrity

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

NOTE: In the event of Cryptographically Relevant Quantum Computer being available provisions under crypto-agility (see clause 4.4) should ensure that the ICV remains strong if the algorithm, or its output length, needs to be changed.

Table 1: Integrity requirements for data transfer

Id	Text of requirement	Status M/O/C (see note 5)
Req-6.1.1	The transmitting device shall provide proof of integrity of signalling mode messaging between devices and the presence of the integrity check value clearly indicated.	M
Req-6.1.1a	All received messages with an integrity check value shall be verified to determine if the message integrity is intact.	M
Req-6.1.1a.1	If the integrity check fails the message shall be discarded.	M
Req-6.1.1a.2	If req-6.1.1a.1 applies the receiving entity shall raise an exception notification to the security reporting entity (see [3]).	M
Req-6.1.2	The message integrity shall be measured over the immutable content of the message (i.e. any mutable content such as hop counters shall not be included in the calculation).	M
Req-6.3	In order to prevent replay attacks each protected message should contain a time-variant or randomized parameter in the scope of the integrity calculation as an anti-replay protection parameter.	R (see note 1)
Req-6.3.1	If the anti-replay parameter is present on receipt the receiving entity shall verify the validity of the anti-replay protection parameter.	C (see note 2)
Req-6.3.2a	If receiving party determines that the message may be replayed, the message shall be discarded.	M C
Req-6.3-2b	If req-6.3-2a is true the receiving entity shall raise an exception notification to the management entity.	M C
Req-6.4	The algorithm used to determine message integrity shall be identified in the link's security association.	M (see note 3)
Req-6.5	The ON should provide proof of integrity of user traffic.	R (see note 4)
NOTE 1: If ECDSA is used the random element applied to the signature meets this requirement. NOTE 2: The granularity of the anti-replay protection parameter has to be sufficient to capture replay. Therefore if a timestamp is used the timestamp has to be of greater granularity than the transmission period between messages. NOTE 3: The provisions for crypto-agility and quantum safe cryptography outlined in ETSI TS 103 924 [1] apply. NOTE 4: Integrity of user traffic is only identified as optional as it may negatively impact the end-to-end delay of user traffic if every traffic packet has to have the integrity check calculated on transmission and verified on receipt. NOTE 5: The status column indicates M as a Mandatory requirement (indicated by shall), C as conditional requirement (if the provision is deployed the means to deploy it are subject to mandatory requirements), R as a recommendation (indicated by should).		

EXAMPLE 1: If using SNMP over TLS then TLS and SNMP profiles exist that achieve all of the above requirements (see bibliography).

EXAMPLE 2: If messages can be sent/received once every second then the granularity of a timestamp used to provide replay protection should be of the order of 0,1 s at least.

EXAMPLE 3: If a sequence counter is used to provide replay protection then the counter should be of sufficient size that it is unlikely to rollover and cause a false replay notification during the normal operation of the system.

NOTE: The content of the table 1 is replicated in Annex A in a simplified ICS format.

6.2 General provisions - confidentiality

The details of the cryptographic algorithm used to protect the confidentiality of data are not defined in the present document, although the boundary conditions and core requirements are stated.

NOTE: If the device supports XGS-PON the provision of XGEN payload encryption as defined in Annex C.15.4 of Recommendation ITU-T G.9807.1 [6] applies.

All transmissions made from the OLT towards the network should be protected by a confidentiality security association. Where used the security association should identify:

- The encryption algorithm.

- The mode used for application of the algorithm (counter mode (CTR), Galois Counter Mode (GCM), etc.) (see ETSI TS 102 165-2 [8]).
- 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.

7 Secure data storage on Optical access network devices

7.1 General provisions

For protection of management and configuration data the provisions of ETSI TS 103 961 [3] apply (see also clause 4.3 of the present document).

Every access device shall have a Root of trust for Storage (RtS) (see for example [i.1] and [i.2]). The present document defines, in this clause, the specific data to be maintained in the RtS.

For an access device there should be independent RtSs for the user/client side and for the network side of the device.

The following characteristics shall be met by the secure storage element:

- Tamper resistant.
- Tamper evident.
- Persistent.

7.2 Access control in OAN devices

The provisions identified in ETSI TS 103 924. Clause 7.2 [1] apply with the additional detailed provisions identified in the present document (see also Annex B).

All data in OAN devices shall be made available to authorized entities using the principle of least privilege (see NIST SP 800-160 Vol.1 Rev.1 [i.5], ISO/IEC 27002 [i.6]). The access control mechanism shall follow the policy model outlined in ETSI TS 102 165-2 [8]. Access control for devices operating in the same trust domain can implement Discretionary Access Control but in general all access control should implement the Mandatory Access Control model (see ETSI TS 102 165-2 [8]).

NOTE 1: As an OAN exists in two domains (network domain and client domain) care should be taken to ensure data unique to one domain should not be accessible from the other.

NOTE 2: Where the OAN client domain serves more than one customer (e.g. the multi-occupancy scenarios shown in Annex E) each distinct client data should not be accessible from any other (see also Clause 4.3 of the present document).

Consistently with ETSI TS 102 165-2 [8] the OAN 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 [3] and where Permission is evaluated using the set model identified in ETSI TS 102 165-2 [8] 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 [3]) (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 OAN 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 OAN device, in collaboration with the ONDS-M, shall set a reporting threshold for making an exception report.

NOTE 3: It is assumed that all functional and data assets of the OAN 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 4: 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 5: The access control model described is similar to that of Attribute Based Access Control (ABAC) 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).

7.3 Access Control rules for OAN devices

The following rules shall be implemented in OAN 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 whose attributes match a pre-configured attribute pattern shall be able to connect to the OAN device (access allowed rule):

- 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 OAN device is configured to reject all management terminal expect the one matching the IP or MAC address pre-configured on the OAN device.

Rule PAC-AC descriptive format: Packets whose configuration maps to pre-configured attribute pattern or value set of attributes shall be dropped (access denied rule):

- 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 OAN device is configured to reject all network packets matching the IP or MAC address pre-configured deny list on the OAN device.

7.4 Access control policy in OAN 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 (see figure 5).

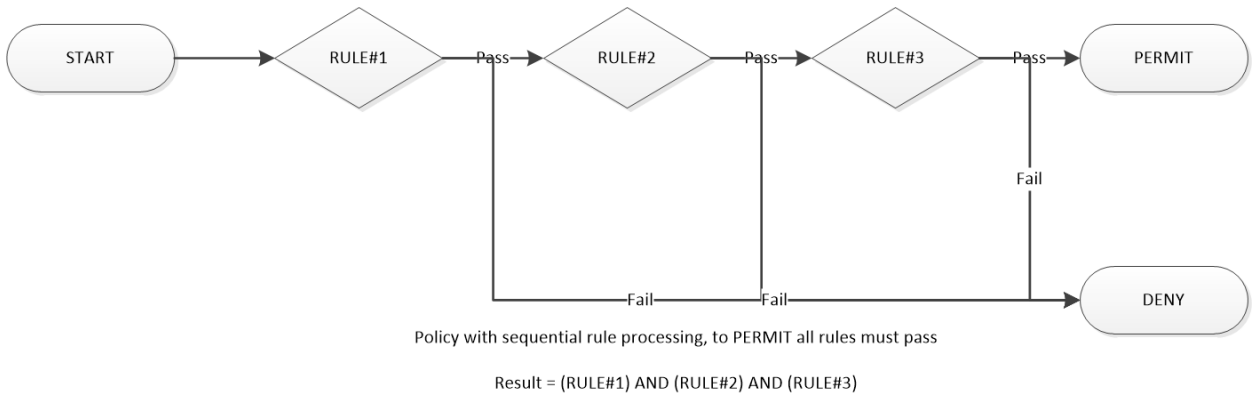

Figure 5: Access control combining rules (attribute settings) where all rules have to pass

Annex A (normative): Simplified ICS Proforma for OAN Device security

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 proforma 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 [5] by the addition of the requirements specified in the present document for the OAN 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 OAN 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 1: 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 OAN Device security

Item	Requirement	Status	Support	Details
Req-1	An access device shall distinguish and keep separate the user and network domains in the device.	M		
Req-2	ON systems shall be designed to be secure by default and to support the functionality required by the CIA paradigm	M		

Item	Requirement	Status	Support	Details
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		
Req-4	Any link enabled during, and post-initialization, shall support periodic re-establishment of the security association.	M		
Req-5	The principles of least privilege and least persistence shall apply to all security associations.	M		
Req-6	In accordance with the least persistence principle security associations shall not be maintained for longer than required.	M		
Req-7	If any software verification fails that software and any supporting elements shall not participate in any security association.	M		
Req-8	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 OAN device shall be integrated to the wider ON and telecommunications system of which it is a component.	M		
Req-10	An OAN device shall consist of at least 1 (one) execution environment.	M		
Req-11	An OAN device's execution environment shall have 1 (one) initial root of trust.	M		
Req-12	The execution environment shall have at least one executable code block.	M		
Req-13	There should be a discrete execution environment for each side and discrete roots of trust for each side.	R		
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		
Req-15	The OAN Device shall have a root of trust used for initialization to enable secure boot capabilities.	M		

Item	Requirement	Status	Support	Details
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		
Req-17	The guidelines given in NIST SP 800-164 [i.2] shall be followed in order to provide the following local (device specific) trust services: Root of Trust for Storage (RTS); Root of Trust for Verification (RTV); Policy Enforcement Engine.	M		
Req-18	The manufacturer of the OAN Device shall attest to the provision of the root of trust by reference to the method applied.	M		
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		
Req-20	The presence of the hardware root of trust shall be asserted by a platform specific attribute certificate.	M		
Req-21	All cryptographic modules shall be designed to be crypto-agile.	M		
Req-22	The specific cryptographic algorithms for each security association shall be defined by the security policy.	M		
Req-23	Cryptographic algorithms should be sufficient to inhibit known cryptanalysis attacks and mechanisms.	R		
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		
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		
Req-26	All ON devices shall be identified with a canonical/root identity and, optionally, additional semantic identifiers identifying their functional nature.	M		
Req-27	Where provided, the semantic identifier shall be used to indicate the functional nature of the entity.	M C		

Item	Requirement	Status	Support	Details
Req-28	The attestation of function shall be verifiable by reference to a 3rd party.	M		
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		
Req-30	The to be authenticated identity shall be an attribute of the authentication protocol.	M		
Req-31	The identity shall always be authenticated on first presentation and periodically thereafter.	M		
Req-32	In order to be consistent with the principle of least persistence an authenticated session shall expire after a set time.	M		
Req-33	The length of an authentication session shall be set by the Authentication-Session-Time-Limit variable.	M		
Req-34	The Authentication-Session-Time-Limit variable shall be established for each security association.	M		
Req-35	A device shall be identified in order to be admitted to the operator's trust domain.	M		
Req-36	Within the trust domain the trust domain manager shall verify the capability of each device.	M		
Req-37	An ON device shall present an identifier to each of the client and the network side of the device.	M		
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		
Req-39	Any identifier presented by the device shall be authenticated by the receiving device.	M		
Req-40	A key shall be associated to an attribute or identifier of the OAN Device.	M		
Req-41	The binding of key to the attribute or identifier shall be maintained for each security association.	M		
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		

Item	Requirement	Status	Support	Details
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		
Req-44	The MAC approach to authentication as outlined in ETSI TS 102 165-2 [8] shall apply.	M		
Req-45	Random challenges used in any MAC based authentication shall be generated using a true source of randomness.	M		
Req-46	Software only functions shall not be used to generate random challenges.	M		
Req-47	A challenge-response method should be used at initialization and for key establishment, key refresh, events.	R		
Req-48	Only cryptographically relevant challenge response schemes shall be used.	M		
Req-49	The challenge response approach to authentication as outlined in ETSI TS 102 165-2 [8] shall apply.	M		
Req-50	Random challenges used in any challenge-response protocol shall be generated using a true source of randomness.	M		
Req-51	A device should only be able to perform a self-attestation of its identity at initialization.	R		
Req-52	The self-attestation shall be provided in the form of a digital signature and include a signed public key.	M C		
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		
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		
Req-55	The OAN device shall have a root of trust for storage to store private cryptographic material (private key).	M		

Item	Requirement	Status	Support	Details
Req-56	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-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		
Req-58	A device should only be able to perform a self-attestation of its capability at initialization.	R C		
Req-59	The self-attestation shall be provided in the form of a digital signature and include a self-signed public key.	M C		
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		
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		
Req-62	All exchanged discrete messages shall have their integrity verified on reception at the device.	M		
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		
Req-64	Any message that fails the integrity check shall be discarded and an error reported.	M		
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		
Req-66	All transmissions made from the OLT towards the network should be protected by a confidentiality security association.	R		

Item	Requirement	Status	Support	Details
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		
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		
Req-69	Every access device shall have a root of trust for storage (RtS).	M		
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		
Req-71	All data in OAN devices shall be made available to authorized entities using the principle of least privilege.	M		
Req-72	The access control mechanism shall follow the policy model outlined in ETSI TS 102 165-2 [8].	M		
Req-73	Each protected Object in the OAN device shall be protected by an access control policy	M		
Req-74	The access control policy shall be evaluated on each access attempt.	M		
Req-75	The policy shall consist of 1 or more rules each of which shall be evaluated in turn.	M		
Req-76	Every denied access attempt shall be recorded.	M		
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		
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		

Item	Requirement	Status	Support	Details
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		
Req-80	If an exception is raised it shall include the details of the rule that failed.	M		
Req-81	The default access control condition for all objects shall be "do not allow"/"do not permit".	M		
Req-82	The following rules shall be implemented in OAN devices: • CFG-AC; • CK-AC; • DEV-AC; • PAC-AC.	M		
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		
Req-84	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 documents referred to in ETSI TS 103 924 [1] that are found in Table B.1 have been suppressed in the 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 [3] 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 5.2.1.2 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 [9] and using the model of non-determinism from NIST SP 800-90B [10].	See clause 5.2.1.3 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.

Source in ETSI TS 103 924 [1]	M/O/C	Applicable text	Provision in 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 7
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 5.2.2.1 and clause 5.2.2.3 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 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 [8]. 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 [i.7], 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 [6]) 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 [6] 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 OAN 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 OAN device

Reference	Requirement	Liable party
R-ENV-1:	The OAN shall be installed in such a manner that any interference with the OAN 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 OAN 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 OAN 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 [5] 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 OAN device should follow best practices, including addressing the requirements in ETSI EN 303 645 [5], in ETSI TS 103 848 [4], and the following shown in table C.2.

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

Reference	Requirement	Liable party
R-DEV-01	Devices shall be developed in such a manner that only essential functions 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.3]).	See note 4
R-DEV-05	Devices shall validate the source and integrity when updating system software.	Development authority
R-DEV-06	Devices should be developed with defensive programming methods 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.5]. 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.5] 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 in table C.3 and table C.4 for each of security auditing and logging, vulnerability reporting (in addition to the general requirements in ETSI TR 103 838 [i.3]).

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 ON access equipment on the market

Within the EU context an OAN device is a device containing digital elements and therefore the Cyber Resilience Act (CRA) [i.14] will apply. For the US market context the provisions of the Cybersecurity Framework [i.15] apply.

Where any user data is gathered and maintained on the OAN device the scope of use of such data is subject to the constraints of the General Data Protection Regulation (GDPR) [i.16]. 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 OAN device should, by default, not contain any user identifying data but this should be confirmed in stage 1 of a Data Privacy Impact Assessment (DPIA).

Annex E (informative): Deployment scenarios for ON access equipment

A number of deployment scenarios for ON access and network devices in the context of Passive Optical Networks (PONs), and for higher speed, are shown in Figure E.1, with services illustrated in Table E.1.

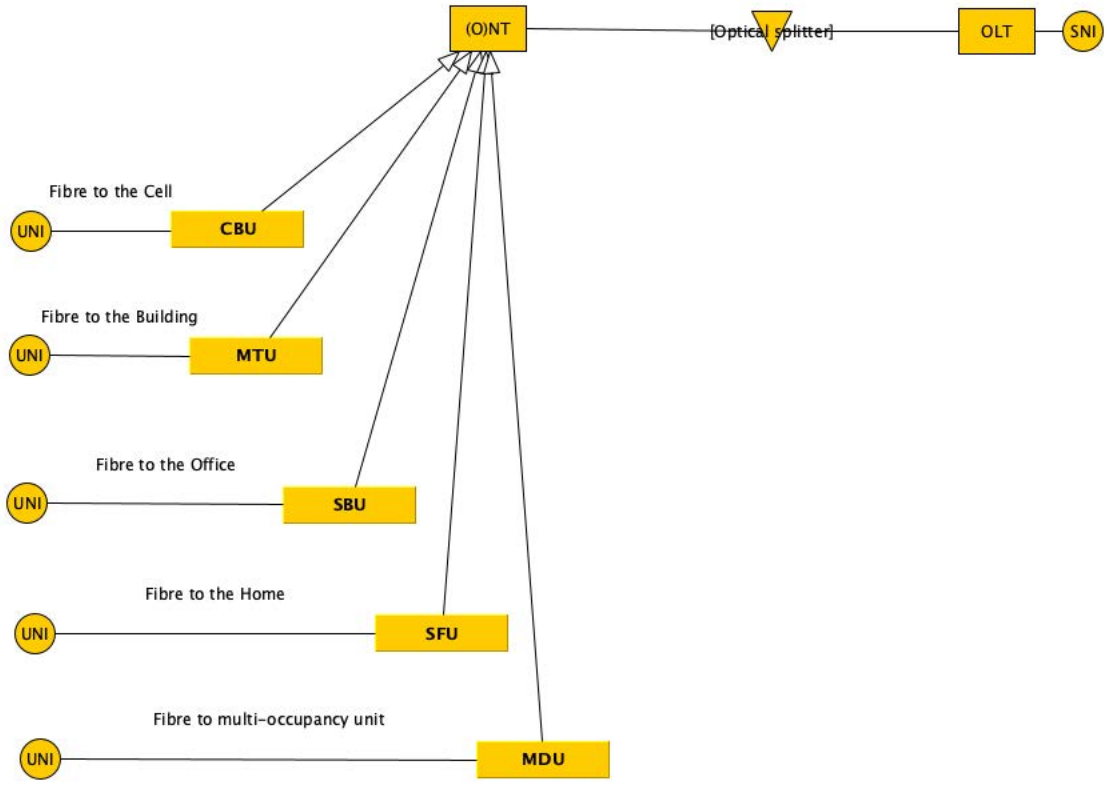

Figure E.1: Deployment scenarios of higher speed PON

For each deployment scenario a number of service categories are identified in Table E.1.

Table E.1: Service Categories supported in higher speed PON scenarios

Scenarios	Services categories
Fibre To The Building (FTTB) (for MDU-served residential users)	• Asymmetric broadband services (e.g. Internet protocol television (IPTV), digital broadcast services, Video on Demand (VoD), file download, etc.). • Symmetric broadband services (e.g. content broadcast, e-mail, file exchange, distance learning, telemedicine, online-games, etc.). • Plain Old Telephone Service (POTS) - Narrow-band telephone services using either emulation (complete replication of a legacy service) or simulation (providing a service that is almost the same as the legacy service).
FTTB (for MTU-served business users)	• Symmetric broadband. • POTS. • Private line - private-line services (including VPN, VPL) at several rates.
FTTC and FTTCab	• Asymmetric broadband services. • Symmetric broadband services. • POTS. • xDSL backhaul.
Fibre To The Home (FTTH)	• Asymmetric broadband services. • Symmetric broadband services • POTS.
Fibre To The Office (FTTO)	Fibre To The Office (FTTO) addresses business ONU dedicated to a small business customer. The following service categories have been considered: • Symmetric broadband services. • POTS. • Private line.
FTTCell	The ONU in a FTTCell scenario will have to offer connectivity to wireless base stations: • Symmetric TDM services. • Symmetric/asymmetric packet-based broadband services. • Hot spots.
FTTdp (Fibre to the distribution point)	The ONU in a FTTdp scenario will be called a Distribution Point Unit (DPU) that in addition to the FTTB service categories and capabilities may support: • Reverse powering capability with power supplied through the copper drop from the end-user installation. • xDSL or G.fast copper drop UNI. • FTTdp architectures involving DPU are described in b-BBF TR-301.
PON-based 5G Mobile FrontHaul (PON-MFH)	The OLT and ONUs provide transport between the Control Unit (CU) and RU. Ultra-low latency with the use of cooperative DBA function and quiet window reduction for the PON. An interface (named Cooperative Transport Interface or (CTI)) between the 5G scheduler and a PON OLT/scheduler as defined by O-RAN WG 4 group in collaboration with ITU SG15 Q2 group.

Annex F (informative): Bibliography

F.1 Secure network protocols for OLT

IETF RFC 4254: SSH

IETF RFC 4253: SFTP

IETF RFC 3826: SNMPv3

IETF RFC 5953: SNMP over TLS/DTLS

IETF RFC 8446: TLS1.3

IETF RFC 5425: Syslog over TLS

F.2 ETSI work in development at time of writing

ETSI TS 103 486: "CYBER; Identity Management and Discovery for IoT"

History

Document history		
V1.1.1	December 2023	Publication