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.

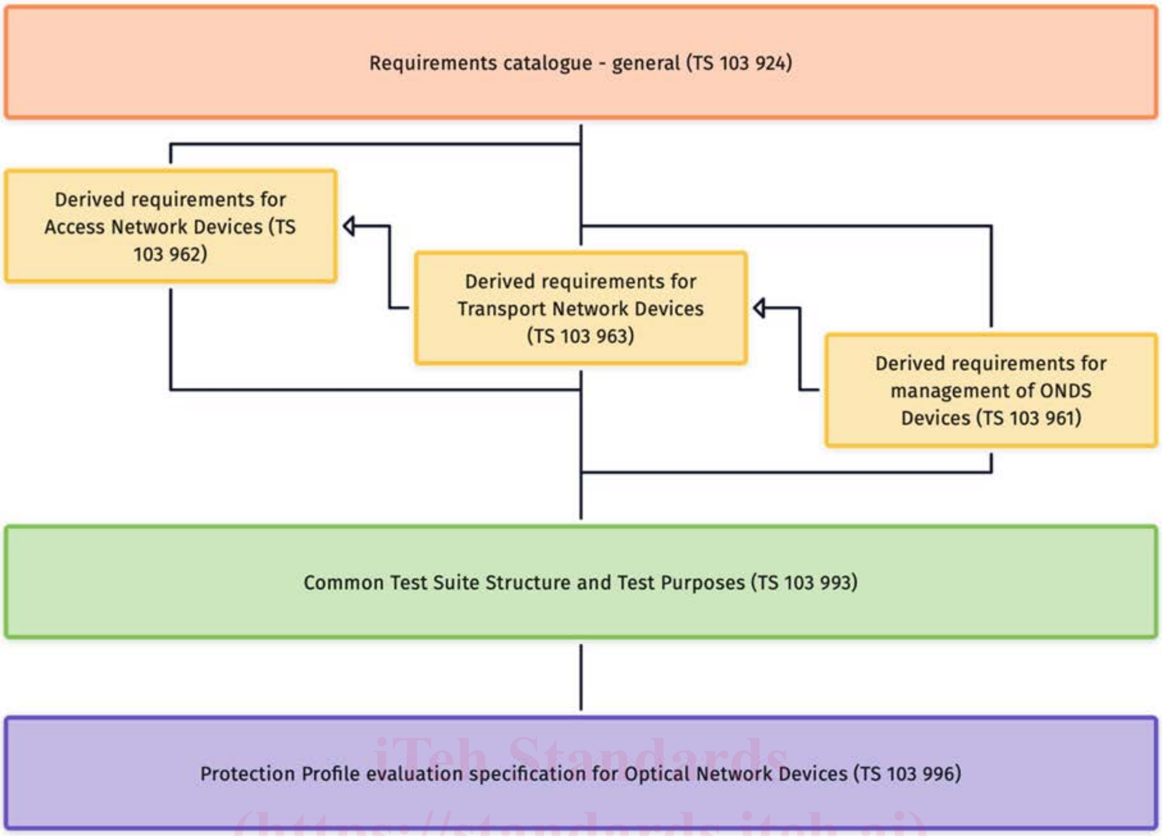

Figure 1: Document structure for Optical Network Device Security

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.

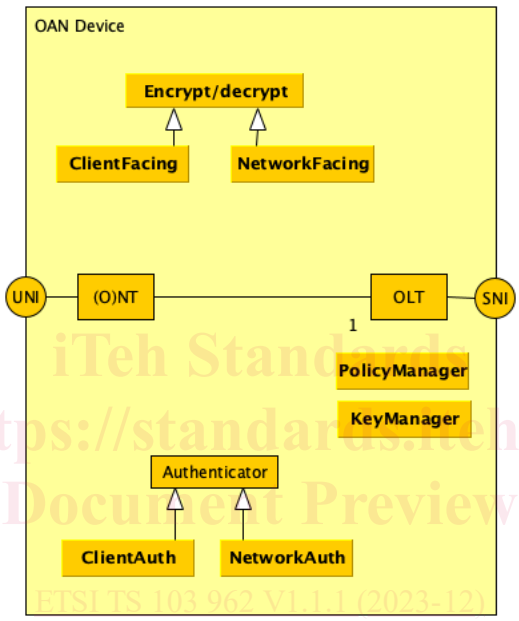

Figure 2: Optical Access Network device

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).

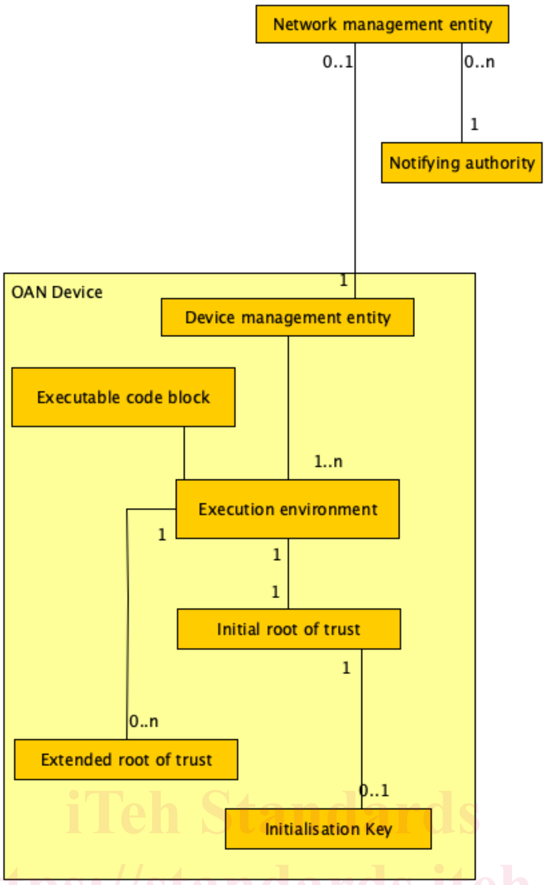

Figure 3: OAN Device functional architecture with respect to security and processing environments

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.