ETSI TS 103 924 V1.1.1 (2022-12)

Optical Network and Device Security
Catalogue of requirements

Reference
DTS/CYBER-0078

Keywords
cybersecurity, network, optical, 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.

1 Scope

The present document provides a catalogue of baseline requirements specific to optical network and devices covering access network, transport network and network management system.

The present document presents the functional requirements using the stage 2 model approach outlined in Recommendation ITU-T Q.65 [i.1] and adopts the functional framework for security functions from ETSI TS 102 165-2 [i.2].

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

[2] FIPS 140-2: "Annex C: Approved Random Number Generators".

NOTE: ISO/IEC 19790:2012: "Information technology - Security techniques - Security requirements for cryptographic modules" (see Annex E, bibliography) also applies for each of [1] and [2].

[3] NIST Special Publication 800-90B: "Recommendation for the Entropy Sources Used for Random Bit Generation".

NOTE: ISO/IEC 20543: "Information technology - Security techniques - Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408" also applies to this standard (see Annex E, bibliography).

[4] Recommendation ITU-T G.975 "Forward error correction for submarine systems".

[5] Recommendation ITU-T G.975.1: "Forward error correction for high bit-rate DWDM submarine systems".

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] Recommendation ITU-T Q.65 (06/97): "The unified functional methodology for the characterization of services and network capabilities".

[i.2] ETSI TS 102 165-2: "CYBER; Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures".

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

[i.4] Broadband Forum..

[i.5] European Parliament legislative resolution of 10 November 2022 on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM(2020)0823 - C9-0422/2020 - 2020/0359(COD).

[i.6] ETSI TS 102 165-1: "CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[i.7] Recommendation ITU-T G.707: "Network node interface for the synchronous digital hierarchy (SDH)".

[i.8] Recommendation ITU-T G.783: "Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks".

[i.9] Recommendation ITU-T G.784: "Management aspects of synchronous digital hierarchy (SDH) transport network elements".

[i.10] Recommendation ITU-T G.803: "Architecture of transport networks based on the synchronous digital hierarchy (SDH)". .

[i.11] ANSI T1.105: "Synchronous Optical Network (SONET) - Basic Description Including Multiplex Structure, Rates, And Formats".

[i.12] ETSI GR ETI 002: "Encrypted Traffic Integration (ETI); Requirements definition and analysis".

NOTE: Currently in development.

[i.13] Recommendation ITU-T G.984.1: "Gigabit-capable passive optical networks (GPON): General characteristics".

[i.14] Recommendation ITU-T X.800: "Recommendation ITU-T X.800: Security Architecture for Open Systems Interconnection for CCITT Applications".

[i.15] Recommendation ITU-T G.805: "Generic functional architecture of transport networks".

[i.16] Recommendation ITU-T G.872: "Architecture of the optical transport network".

[i.17] Recommendation ITU-T G.7714.1: "Protocol for automatic discovery in transport networks".

[i.18] FIPS 197: "Advanced Encryption Standard (AES)".

NOTE: The above specification is also included in ISO/IEC 18033-3 [i.42].

[i.19] FIPS 180-4: "Secure Hash Standard (SHA)".

[i.20] ETSI TR 103 305-1: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.21] ETSI GR F5G 010: "Fifth Generation Fixed Network (F5G); Security; Threat Vulnerability Risk Analysis and countermeasure recommendations for F5G".

[i.22] IETF STD 62.

NOTE: See https://www.rfc-editor.org/info/std62.

[i.23] NIST SP 800-38D: "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC".

[i.24] ETSI GR NFV-SEC 003: "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance".

[i.25] Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive.

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

[i.27] OTN-SEC (Supplement 76 to ITU-T G-Series Recommendations provides an overview of applications and use cases for secure optical transport in various OTN layers. The Supplement relates to Recommendations ITU-T G.709/Y.1331 and ITU-T G.709.1/Y.1331.1).

[i.28] IETF RFC 3414 (STD 62): "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)".

[i.29] ETSI TR 102 419: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security analysis of IPv6 application in telecommunications standards".

[i.30] Recommendation ITU-T G.709.1: "Flexible OTN short-reach interfaces".

[i.31] NIST Framework for Improving Critical Infrastructure Cybersecurity.

NOTE: Available from https://doi.org/10.6028/NIST.CSWP.04162018.

[i.32] Recommendation ITU-T G.9807.1: "10-Gigabit-capable symmetric passive optical network (XGS-PON)".

[i.33] Recommendation ITU-T M.370x: "Common management services".

NOTE: 'x' refers to all of M.370/M.3701/M.3702 and so on.

[i.34] Recommendation ITU-T G.7710: "Common equipment management function requirements".

[i.35] Recommendation ITU-T G.984.3: "Gigabit-capable passive optical networks (GPON): Transmission convergence layer specification".

[i.36] Supplement 51 to Recommendation ITU-T G-series: "Passive optical network protection considerations".

[i.37] Recommendation ITU-T G.987: "10-Gigabit-capable passive optical network (XG-PON) systems: Definitions, abbreviations and acronyms".

[i.38] Recommendation ITU-T G.989: "40-Gigabit-capable passive optical networks (NG-PON2): Definitions, abbreviations and acronyms".

[i.39] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.

[i.40] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance).

[i.41] ETSI TR 103 838: "Cyber Security; Guide to Coordinated Vulnerability Disclosure".

[i.42] ISO/IEC 18033-3: "Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

adaptation source: transport processing function which adapts the client layer network characteristic information into a form suitable for transport over a trail in the server layer network

Control Plane Security Function (CPSF): set of security functions that protect activities that enable the efficient exchange of control and signal data

NOTE: The CPSF typically involves Network Element (NE) to NE communication of information that allows NEs (e.g. OTN, OLT) to determine how best to transfer traffic across the optical transmission network.

General Security Function (GSF): set of general security functions that apply to UPSF, CPSF and MPSF to provide fundamental protections for optical NEs

Management Plane Security Function (MPSF): set of security functions that protect OAM&P functions of the optical NEs

Optical Transport Network (OTN): optical telecommunication network segment comprised by a set of optical network nodes/equipment connected through optical fibres that provide the functionality of transport, multiplexing, switching, management, supervision and survivability of the optical channels carrying the end-user's client signals, according to the requirements given in Recommendation ITU-T G.872 [i.16]

Optical Transport Network Node Interface (ONNI): interface at an optical transport network node which is used to interconnect with another optical transport network node

trail: "transport entity" which consists of an associated pair of "unidirectional trails" capable of simultaneously transferring information in opposite directions between their respective inputs and outputs (from Recommendation ITU-T G.805 [i.15])

User Plane Security Function (UPSF): set of security functions that secure the connectivity provided by carriers, user access and use of the network, the user data flows transferring via optical network

3.2 Symbols

Void.

3.3 Abbreviations

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

ABAC	Attribute Based Access Control
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
AON	Active Optical Network
CBA	Cost Benefit Analysis
CIA	Confidentiality Integrity Availability
C-MAC	Cipher-based Message Authentication Code
CPE	Customer Premises Equipment
CPN	Customer Premises Network
CPSF	Control Plane Security Function
CRC	Cyclic Redundancy Check
CSC	Cyber Security Control
DCN-DA	Data Centre Network Discovery Agent
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DMARC	Domain-based Message Authentication Reporting and Conformance

DNS	Domain Name System
DoS	Denial of Service
FCAPS	Fault Configuration Accounting Performance Security
FCC	Fast Channel Change
FEC	Forward Error Correction
FTTB/C	Fibre To The Building/Curb
FTTCab	Fibre To The Cabinet (data centre cabinet)
FTTH	Fibre To The Home
GEM	GPON Encapsulation Method
GPON	Gigabit capable Passive Optical Networks
GSF	General Security Function
HMAC	Hash based Message Authentication Code
HTML	Hypertext Markup Language
HTTP/S	HyperText Transfer Protocol / Secure
IP	Internet Protocol
IV	Initialization Value
MAC	Message Authentication Code
MFA	Multi-Factor Authentication
MFAS	Multi Frame Alignment Signal
MPLS	Multi Protocol Label Switching
MPSF	Management Plane Security Function
NE	Network Element
NG	Next Generation
NIDS	Network Intrusion Detection System
NMS	Network Management System
NMS-EMS	Network Management System - Element Management System
O&AM	Operations and Asset Management
O&M	Operations and Management
OAM&P	Operations, Asset Management and Provisioning
OAN	Optical Access Network
ODU	Optical Data Unit
OH	OverHead
OLT	Optical Line Terminal
OMCI	Optical network terminal Management and Control Interface
ON	Optical Network
ONNI	Optical transport Network Node Interface
ONT	Optical Network Termination
ONU	Optical Network Unit
OPU	Optical Payload Unit
OSI	Open Systems Interconnection
OSMC	OTN Synchronization Message Channel
OTH	Optical Transport Hierarchy
OTN	Optical Transport Network
OTU	Optical Transport Unit
PCEP	Path Computation Element
PLOAM	Physical Layer Operation Administration and Maintenance
PON	Passive Optical Network
RoT	Root of Trust
RS	Reed Solomon
SA	Security Association
SDH	Synchronous Digital Hierarchy
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SPL	SPLitter
TCP-ID	Termination Connection Point Identifier
TCP-ID	Termination Connection Point Identifier
ToE	Target of Evaluation
UPSF	User Plane Security Function
URL	Uniform Resource Locator
USM	User-based Security Model
WDM	Wavelength Division Multiplexing
XGS	10-Gigabit-capable Symmetric PON (in the context of XGS-PON)

4 Summary of security requirements for optical networks and devices

4.1 Rationale for provision of security functions in optical networks

Optical fibre networks are not immune to security attacks. The splicing of optical fibre and the leakage of signals from bent fibres is a recognized means of extracting content from fibre thus the confidentiality of communications without additional measures cannot be assured. Similarly it is possible for an attacker to inject signals into fibre and therefore the source and integrity of any signal or content can similarly not be assured. A simplified threat evaluation is given in Annex A of the present document. It is necessary to consider that optical networks are targets of attack and that assurance of confidentiality, integrity and availability cannot be given without added security measures.

A number of techniques do exist for detection of faults that can indicate a potential breach. For example if the cable is distorted or damaged at a splice point, or interception curve, optical reflectometry can detect the approximate location of the breach. However as the optical bandwidth is increased, and the symbol rate is increased, the noise margin of the connection is decreased with the result that adding probe signals to detect line problems may interfere with the signal by further reducing the noise margin. The degree to which an interception probe interferes with the optical transport signal is not fixed and can, if applied, result in loss of signal at the receiver.

NOTE 1: As identified in a number of sources (see Annex E, bibliography) the tapping of optical fibres to extract content is a well known attack vector for interception of content.

NOTE 2: The term interception is often considered to be a synonym of the term eavesdropping to imply secretly "listening in" to the content of communication. The term interception as used in the present document is more nuanced and is intended to convey the act of finding and observing where communication takes place, i.e. the fibre optic cable. Any action after interception, such as listening in or eavesdropping on content, is considered for the present document as a secondary action and unrelated to the interception itself.

4.2 Definition of optical network

An optical network is distinguished from a non-optical network by the physical means of transferring data, which is achieved using fibre optic links, data encoded using photons, and by the use of optical switching. The core definition of the structure of Optical Networking interfaces is found in Recommendation ITU-T G.709 [i.3], defining the Optical Transport Hierarchy (OTH), including the structure of an optical data unit, which is revised and extended by activities of other ETSI groups and by groups including the Broadband Forum [i.4]. The core definition of the structure of Gigabit capable Passive Optical Networks (GPONs) is found in Recommendation ITU-T G.984.1 [i.13], defining the network architecture, reference configuration, interfaces and so on.

For the purposes of the present document the optical network is defined as a network that lies between the customer premises network and the core network with a primary purpose of providing high-capacity data access and high-rate data transport to enable high-quality network services with full fibre connection. For the present document the term optical network is limited to considerations of the Optical Transport Network (OTN) and the Optical Access Network (OAN) and to the devices that support them. It provides network access and transport services to a variety of markets including individual customer, government, industry, business, etc. Thus the present document discusses the optical access-, aggregation- and core network aspects.

NOTE 1: The core content of Recommendation ITU-T G.709 [i.3], nor of Recommendation ITU-T G.984.1 [i.13], does not define any security specific elements or any encoding of native security functionality.

Historically the Synchronous Optical Network (SONET) and the Synchronous Digital Hierarchy (SDH) also played a significant role in the delivery of optical networking services for (mostly) circuit mode connections (voice) and the latter was developed in ETSI but later subsumed into standards from ITU-T as Recommendations G.707 [i.7], G.783 [i.8], G.784 [i.9] and G.803 [i.10]. The SONET specification is formalized in ANSI T1.105 [i.11]. The present document focusses on the mapping to OTH and to GPON, and only addresses SDH and SONET for completeness as mappings exist for carriage of SDH/SONET on OTH.

NOTE 2: SONET, SDH and G.709 all refer to themselves as transport protocols but this is not to be confused with the transport layer protocol model commonly identified in the OSI model. The model in SONET, SDH and G.709 applies transport to the physical means of getting data from A to B across a network using an optical transmission system (i.e. fibre optic cable and phased light), i.e. transport protocol in the meaning of transmission protocol.

NOTE 3: OTN as defined in Recommendation ITU-T G.709 [i.3], operates at the data link layer (i.e. layer 2) of Open Systems Interconnection (OSI) model defined in Recommendation ITU-T X.800 [i.14] thus whilst referring to Optical Transport Networks this should not be confused with the functions of the OSI transport layer.

The optical information elements in OTH (G.709) represent one of control, signalling data, and user data. The distinction between control data and signalling data is that control data is required by the system itself to manage entities in the optical network (e.g. O&M facilities), whereas signalling data is associated to the user plane. In addition the user data plane can contain higher layer signalling that is transparent to the optical network.

EXAMPLE: User devices connecting to the Internet and to Web-services will exchange a number of signalling protocols including DNS, HTTP/S and SNMP that present data to user applications in the form of URLs, HTML pages and email content.

It is recognized that the telecommunications network is composed of a mix of optical links, copper links (e.g. twisted pair or coaxial cable ethernet links), wireless links (long and short range), and silicon based processing. An attack on an associated processing element or copper link or wireless link can be considered as a side-channel attack on the optical fabric. It is also recognized that an attacker can use multiple attacks in sequence or in parallel to achieve their goals. A summary of the threats and vulnerabilities associated to ONs is given in Annex A of the present document.

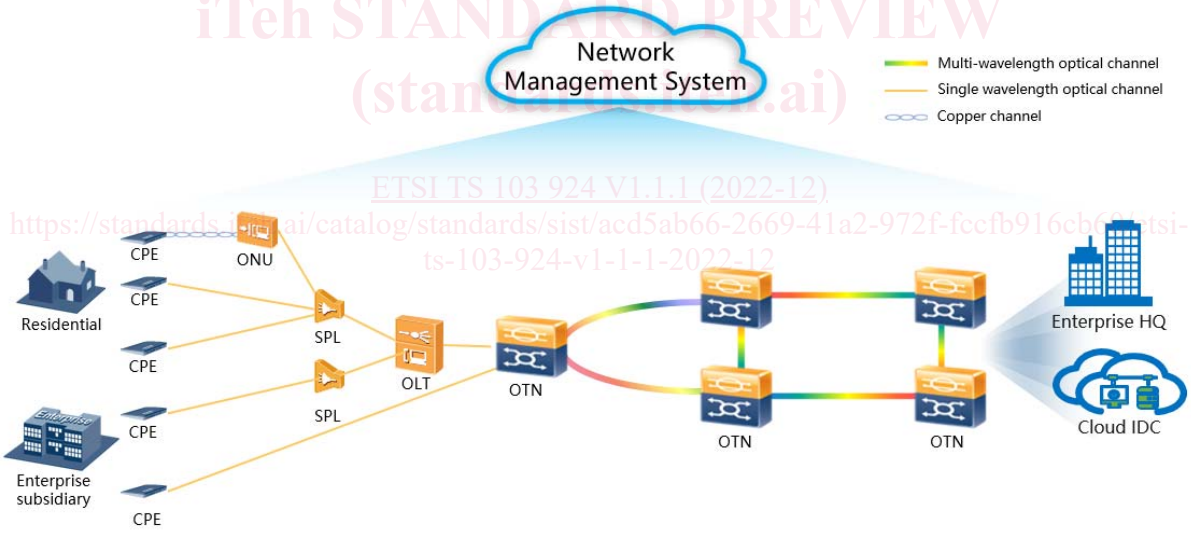

Figure 1: Optical network architecture (device level)

4.3 Optical network functionality (user and control)

NOTE 1: The text in this clause summarizes functions in optical networks that is derived from G.709, SDH and SONET.

The optical network in the scope of the present document describes a transmission system that is used to carry client data, where client data can be presented in a number of formats, including Ethernet frames, IP packets, MPLS frames and so on. Client data is transferred through the Optical transport network by encapsulation into an Optical Payload Unit (OPU) into an Optical Data Unit (ODU), or directly as an OPU. OPUs are then encoded into Optical Transport Units (OTUs). The point of interconnect between nodes is identified by the Optical Network Node Interface (ONNI) which is defined in detail in Recommendation ITU-T G.805 [i.15], and also in Recommendation ITU-T G.709 [i.3], and is derived from the functional architecture defined in Recommendation ITU-T G.872 [i.16].