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.

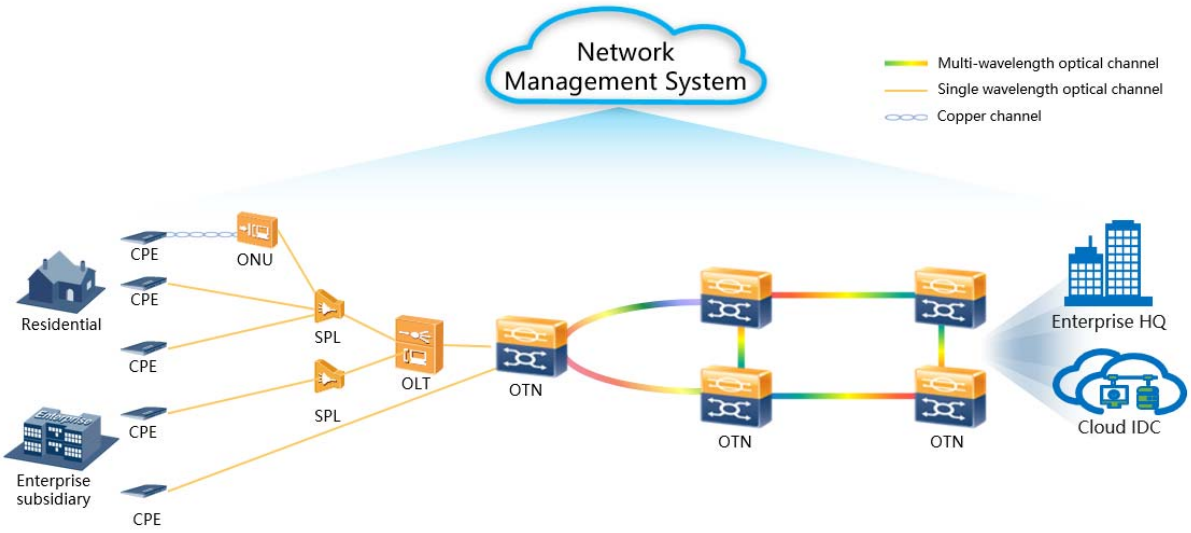

Figure 1: Optical network architecture (device level)

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].

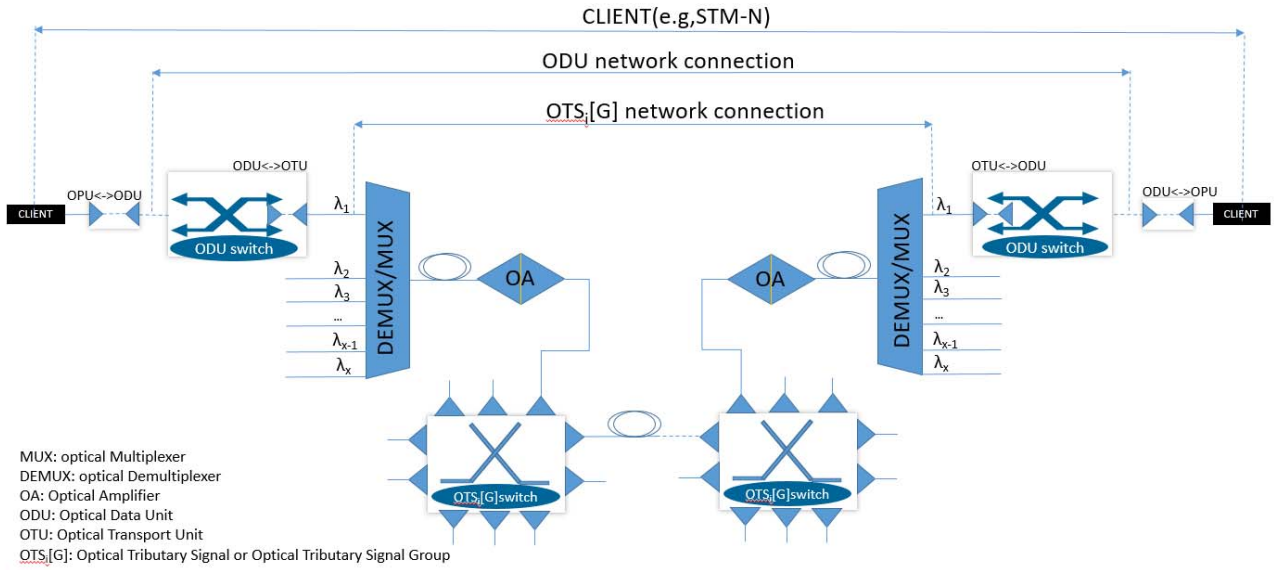

Figure 2: Optical Transport Network Connection structure

In general terms an optical network consists of 2 types of physical network device: Optical Line Terminal (OLT) and Optical Transport Network switches or routers (OTN).

NOTE 2: The OLT, OTN distinction can be derived from the functional model given in Recommendation ITU-T G.805 [i.15] where the OLT is an adaptation source of a trail.

NOTE 3: The combination of function into specific devices is not addressed by the present document although in the present document indicative combinations are presented in Annex A.

As seen in figure 1 "Network architecture" in clause 5.1 of Recommendation ITU-T G.984.1 [i.13] the OAN, an optical implementation of a local access network system, can be either active or passive and its architecture can be either point-to-point or point-to-multipoint. Figure 1 of the present document shows the architectures considered of a local access network system, which range from Fibre To The Home (FTTH), through Fibre To The Building/Curb (FTTB/C) to Fibre To The Cabinet (data centre cabinet) (FTTCab), and practically to a room or client device. Client data processed by an OLT will be transmitted into the OTN.

4.4 Optical network functionality (management)

The provisions for securing the management of the optical network should follow existing best practice for securing management data and protocols.

In particular it is recognized that the NMS manages and controls devices on optical networks, supports unified management, and offers control of networks. Thus the NMS integrates functions including network management, service control, and network analysis. It is enablement system for network resource pooling, network connection automation and self-optimization, and O&M automation. The Recommendation ITU-T M.370x [i.33] series of Recommendations define the management functions applicable in the Network Management System-Element Management System (NMS-EMS) interface which includes object management, state management, notification management, performance management and fault management. More specifically, the common equipment management function requirements for optical network are specified in Recommendation ITU-T G.7710 [i.34]. The optical NMS can support SNMP, PCEP, and Netconf, with the following functionalities:

- discover and update the network topology in real time;
- conduct the device and service configuration;
- FCAPS management;
- responsible to the network resilience via mechanisms like protection and/or restoration.

EXAMPLE: If Simple Network Management Protocol (SNMP), defined in IETF STD 62 [i.22], is used then the security models incorporated are adopted, thus the User-based Security Model (USM) defined in IETF RFC 3414 [i.28] are used.

4.5 Optical network security objectives

It is noted in [i.5] that optical networks are susceptible to eavesdropping attacks by interception of the signals on the fibre, and have associated vulnerabilities of availability from conventional physical attack. It is also noted that as the data load carried by optical networks is substantial, and that a single fibre using the multiplexing arrangements described in Recommendation ITU-T G.709 [i.3] support multiple customers and/or multiple services, an attack of any type will have a high impact to the customer. (See also the risk analysis provided in Annex A).

NOTE 1: When the term optical transmission is used in the present document it is referring to the physical use of light to transfer data and not to any specific network configuration or equipment.

As stated in ETSI TS 102 165-1 [i.6] an objective is the expression of what a security system should be able to do in very broad terms, whereas a requirement is a more detailed specification of how an objective is achieved.

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.

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).

Data (content, control, signalling) that is essential to the management of the network **should** only be visible to authorized entities in the network.

NOTE 2: The capabilities defined in ETSI GR ETI 002 [i.12] apply where encryption is applied to data.

Clauses 5, 6, 7 and 8 introduce general requirements to achieve the security objectives.

4.6 ON (user, control and management) security and trust associations

In like manner to the model given in ETSI TS 102 165-2 [i.2] each security measure creates a security association between two or more assets in the ON (see also Annex D). The security association can also be dependent on an explicit trust association that creates a trust boundary around a set of assets (the set of assets within the trust boundary is considered to be in the same trust domain (see also Annex D)).

5 Identification and authentication framework

5.1 Introduction

In simple terms identity, semantic or canonical, in context, is the anchor for most security functions if a key or credential is bound to an identified entity and purpose.

NOTE: A semantic identity is one that informs of its purpose, so an email address is a semantic identifier as it informs that the content is for use in email. A canonical identifier is one that has no association to purpose but where its purpose is added by an association, an example is the string 123456 which if used as an identifier needs additional context to identify its purpose, for example it can be the serial number of an IoT device.

Conventionally at the OSI-Link layer, layer-2 and at the physical layer (layer-1), the set of functions identified by Recommendation ITU-T X.800 [i.14] are as follows:

- At layer 1: Connection confidentiality, Traffic flow confidentiality
- At layer 2: Connection confidentiality, Connectionless confidentiality

With respect to the security functions of the NMS entities, they are mapped to the OSI model at each of the network layer, session layer, presentation layer and application layer, and the set of functions identified by Recommendation ITU-T X.800 [i.14] at layer 3 are as follows:

- At layer 3: Peer entity authentication, Data origin authentication, Access control service, Connection confidentiality, Connectionless confidentiality, Traffic flow confidentiality, Connection integrity without recovery, Connectionless integrity.

Within the optical network, entities shall be able to be uniquely identified to each other element within a single trusted domain (see Annex C for an overview of the establishment of trusted domains in ONs).

For each of Connection confidentiality and Connectionless confidentiality the confidentiality service (see also clause 6) shall be bound to the semantic and canonical identifier of the terminator of the service.

The mechanisms defined in Recommendation ITU-T G.7714.1 [i.17] and in Recommendation ITU-T G.709 [i.3] clause 15.8.2.3 apply for the definition and assignment of a Termination Connection Point Identifier (TCP-ID) that can be used in the context of discovery when combined with a Data Centre Network Discovery Agent identifier (DCN-DA id) (see [i.17] and [i.3] for a complete definition of discovery).

5.2 Functional identification and authentication

An entity is functionally defined by semantics and context. A device has function, e.g. a demultiplexer functions by dividing the WDM path into its non-multiplexed elements, and it has context including its physical location.

The combination of sematic identity, contextual identity and canonical identity uniquely identifies the ON element.

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.

NOTE 1: If confidentiality protection uses an algorithm in Authenticated Encryption with Associated Data (AEAD mode), e.g. AES-GCM, the associated data can form an element for persistent authentication of data (over and above any use of an encryption key derived during the authentication phase). It is possible to use Encrypt-then-HMAC as a means to implement AEAD if sufficient care is taken in implementation, particularly in cryptographic separation of the HMAC and encrypt functions (different key for each function).

NOTE 2: 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.

In the specific context of ON:

- Any random challenges required in the authentication protocol shall be generated using a method as described in Annex C of FIPS 140-2 [1] and [2] and using the model of non-determinism from NIST SP 800-90B [3].

6 Confidentiality protection

6.1 Protection of data in transit (access and core)

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 (see Annex E and ETSI TS 102 165-2 [i.2]) using an appropriate mode (to be identified in future work items).

NOTE 1: It is recognized that at the time of writing the present document that the ITU-T development of OTN-SEC [i.27] is ongoing and should be taken into account on publication.

NOTE 2: The GEM or OPU is the content that is being encrypted and any differences between them for the purposes of the present document is irrelevant.

NOTE 3: Given the nature of transmission it is inevitable that errors in transmission will occur and that for implementation of the encryption mechanism the implementor assumes that errors to the block affected by the transmission are corrected using an appropriate link layer (OSI-L2) mechanism (see the CRC identified in clause 7).

NOTE 4: The very high data transfer rates available in ONs require that care is taken in the setting of any Initialization Vector (IV) value to prevent replay attacks, e.g. for AES GCM as outlined in NIST SP 800-38D [i.23], clause 8.3 "Constraints on the number of invocations".

The CRC defined in Recommendation ITU-T G.975 [4] and Recommendation ITU-T G.975.1 [5] **shall** be applied to the encrypted payload (see also clause 7.2).

The security association for confidentiality protection is link specific (see also Annex D) and operates with the trust domain established for the SA.

EXAMPLE: An SA is established between the CPE and the peer OTN device, where the SA defines AES-GCM for the algorithm, and the security policy identifies the content of the GCM mode authentication data.

6.2 Protection of data at rest

6.2.1 Cryptographic key management (symmetric keying)

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.

6.2.2 Certificate management (asymmetric keying)

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).

EXAMPLE: Acting appropriately on a revoked certificate can include rejecting the data associated to the certificate and raising a security warning to an appropriate authority.

7 Integrity protection

7.1 Core capabilities of OTH

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 [4] 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).

Figure 3: Positioning of CRC and Cryptographic Integrity check (abstract view)

NOTE 1: The encrypted OPU comprises encrypted user data and OPU overhead (there are minor variations in the presentation of user data across the ON standards and the scope of coverage of the FEC/CRC that are not addressed in the present document).

NOTE 2: Reed-Solomon codes can detect and correct multiple symbol errors. By adding t = n - k check symbols to the data, where n is the block length, and k is the message length, a Reed-Solomon code can detect (but not correct) any combination of up to t erroneous symbols, or locate and correct up to $\lfloor t/2 \rfloor$ erroneous symbols at unknown locations.

EXAMPLE: In Recommendation ITU-T G.975 [4] the code RS(1023, 1007) adds 16 symbols to each block of 1 007 symbols to detect and correct up to 8 symbol errors in any transmitted block.

NOTE 3: The FEC mechanism has no security strength but is intended to identify and correct small numbers of transmission errors, and is only considered in the present document as an availability measure to maximize link availability and to give higher confidence in the cryptographic protection modes, identified in clause 6 and in clause 7.3, operating without error.

NOTE 4: In Recommendation ITU-T G.709.1 [i.30] and [i.27], for FlexO it is noted that the FEC CRC-16 (2 bytes) is located in overhead bytes 11 and 12 of each FlexO frame. The CRC protects the integrity of the OH fields in bytes 2 to 10 and excludes the MFAS, OSMC and FCC fields thus does not provide full Forward Error Protection of the transferred packet.

7.2 Network and Data integrity protection in transit

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 [i.14] 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.

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 [i.2]. The C-MAC should use a key derived from the authentication process (see clause 5) and distinct from that used in the confidentiality service (see clause 6).

NOTE: ETSI TS 102 165-2 [i.2] identifies a number of forms of keyed MAC where the way in which the key is applied to the hash varies.

7.3 Integrity protection of data at rest

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.

NOTE: The ON is intended to transfer data and is not expected to store any user level data. The configuration and management data of any ON device is not addressed in this clause.

7.4 Message Integrity Protection

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.35], 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 [i.32]) enhanced integrity protection shall be used using the mechanisms identified in the current clause.

8 Availability protection

8.1 Redundancy protection

The capabilities defined in Recommendation ITU-T G.987 [i.37] series, Recommendation ITU-T G.989 series [i.38], and Recommendation ITU-T G.9807.1 [i.32] 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 [i.36] further develops the specifications and should be applied as appropriate to the specific technology.

8.2 Denial of Service and Distributed Denial of Service protection

The general principles for Denial of Service and Distributed Denial of Service (DoS/DdoS) protection defined in ETSI TS 102 165-2 [i.2] apply.

NOTE: The text in ETSI TS 102 165-2 [i.2] updates text that previously was to be found in ETSI TS 102 165-1 [i.6] and ties it to application of core capabilities also defined in ETSI TS 102 165-2 [i.2].

8.3 Network security awareness

The general principles outlined in the Security Controls defined in ETSI TR 103 305-1 [i.20] apply and are detailed in clause A.4. As indicated in clause A.4 many security processes, functions and actions should be implemented to benefit from the security provisions of the ON/OTN described in the present document.

8.4 Passive versus Active Optical Networks

In a passive network optical couplers/splitters can be used to differentiate/route user traffic. As there is no active amplification of the signal on any PON there is a limit to the number of connections possible before the impact of noise makes communication impossible. In contrast an Active Optical Network making use of amplifiers on the line and switching is less constrained with respect to noise limitation on performance but does require that power is available at the active components.

An active network is susceptible to outage by loss of power, whereas a PON is differently susceptible.

NOTE: A PON does require power to operate, however on the link from the core to the CPE no additional power is required to operate, even at couplers/splitters, whereas an AON requires power at each switch so there are potentially more points of failure in an AON than in a PON.

Annex A (informative): Simplified threat analysis for optical networks

A.1 Overview and method

The NIST framework principles [i.31], alongside the ETSI TVRA method in ETSI TS 102 165-1 [i.6], and the security controls defined in ETSI TR 103 305-1 [i.20] inform the present annex.

The NIST framework principles from clause 2.1 of [i.31] identify a cycle of activities to provide protection (the cycle of Identify - Protect - Detect - Respond - Recover).

NOTE 1: The NIST framework principles identify and strongly recommend several practices that are implemented over and above the technical provisions of the present document. This includes the operator of telecommunication services implementing a vulnerability disclosure and reporting system (see for example ETSI TR 103 838 [i.41]), and adopting reasonable practices in line with the security controls defined in ETSI TR 103 305-1 [i.20] (see clause A.4 of the present document).

NOTE 2: The NIST framework principles are shared between vendor, developer and operator of a system.

Optical Networks, and optical network technologies, are deployed extensively by operators and many vendors/manufacturers already supply equipment that complies to the existing standards suite for GPONs [i.13]. In recognizing this the role of Cost-Benefit-Analysis steps of the TVRA approach are somewhat critical as there may be non-technical risks arising from the deployment of new features that make old or existing network deployments obsolete. However that has to be balanced against the regulatory requirements stemming from the CSA and from NIS2 amongst others that require a balanced approach to security.

A.2 Core risk analysis - asset level risks

The TVRA method in ETSI TS 102 165-1 [i.6] requires that a system under evaluation, the Target of Evaluation (ToE), is decomposed into its assets and the relationships between assets. For reference the analysis of the underlay plane given in ETSI GR F5G 010 [i.21] applies. The ToE for an Optical Network (ON) is, in simplified form, the core model shown in figure A.1.

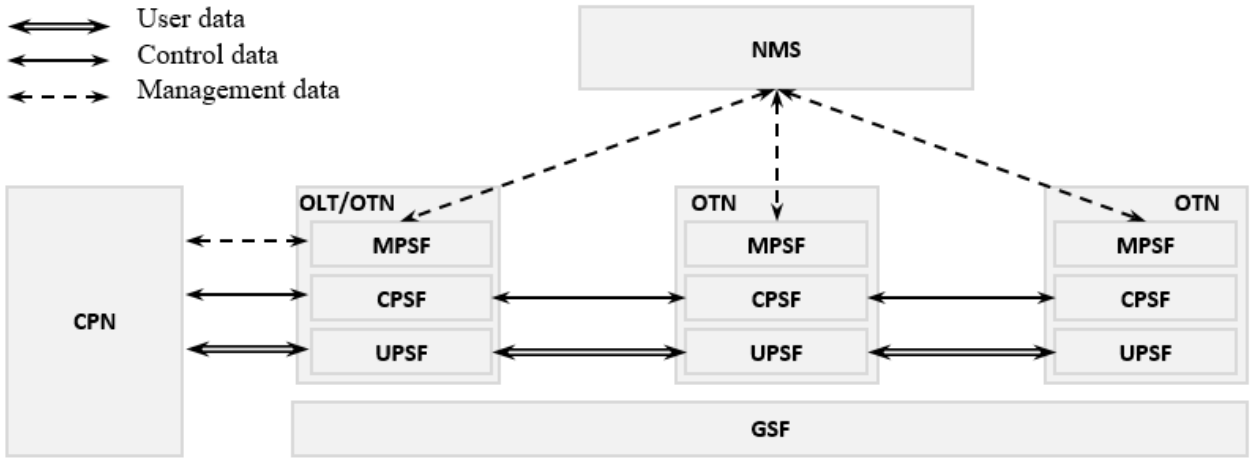

Figure A.1: Optical network architecture (functional level)

It is recognized that an ON, in common with other telecommunications systems, relies upon software to operate and thus the software functions are of themselves assets of the system in addition to, but distinct from, the hardware they run on.

A.3 Cost Benefit Analysis - outline view and application

A.3.1 Standards design

As stated in ETSI TS 102 165-1 [i.6] introducing countermeasures to a standard under development or an existing standard (published) can impose changes affecting the time schedule and resulting in additional effort and cost. In undertaking this analysis for ONs it is recognized that a very significant deployment already exists, and that the existing specifications have only limited mandatory provisions for security. The assigned CBA score is thus medium impact as the application of additional standards, and standards compliance, from the frameworks identified in the present document are not insignificant.

Table A.1: Standards design evaluation

Scale	Description	Assigned value
Medium Impact	Significant time delay and additional resource demand for standards under development and significant changes needed on existing and published standards.	4

A.3.2 Implementation

As stated in ETSI TS 102 165-1 [i.6] adding countermeasures to standards can affect its adoption and implementation in the targeted user community. The considerations given in table A.1 apply equally to implementation.

Table A.2: Implementation evaluation

Scale	Description	Assigned value
Medium Impact	Significant effect on standards adoption in the targeted user community.	4

A.3.3 Operation

Countermeasures can impact the ongoing operation of standardized products or systems once they have been deployed into an operational environment. In the extended facilitation of security measures it is adjudged that the ongoing impact on operations is of relatively low impact. It is assumed in this that the measures described in the body of the present document can be implemented using mature technologies hence the assigned score of "Low impact".

Table A.3: Operation evaluation

Scale	Description	Assigned value
Low Impact	No significant effect on operation of realized standards design or targeted operational environment.	1

A.3.4 Regulatory impact

Regulatory impacts concern the influence that the countermeasure can have on ensuring regulatory compliance. In anticipation of the full impact of RED [i.25], NIS2 [i.5] and the CSA [i.26] where there is greater expectation of security provisions the impact of the framework provisions in the present document are deemed to be likely to lead to a significantly positive impact.

Table A.4: Regulatory impact evaluation

Scale	Description	Assigned value
Positive Impact	Significant positive effect on regulatory compliance requirements.	4

NOTE: Other regulatory regimes can apply in addition to those cited, including the Cyber Resilience Act proposal [i.39], and GDPR [i.40]. The overall assessment remains that taking the measures outlined in the main body of the present document will result in significant positive effect on regulatory compliance requirements.

A.3.5 Market acceptance

As with the assessment of regulatory impact (clause A.3.4) the adoption of the measures defined in the present document suggest, as per table A.5, a significant positive impact on the acceptance of ONs.

Table A.5: Market acceptance evaluation

Scale	Description	Assigned value
Positive Impact	Significant positive effect on market acceptance.	4

A.4 Wider review of application of security controls

ETSI TR 103 305-1 [i.20] 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. For example CSC14, Security Awareness and Skills Training, is essential to the organization developing and deploying ONs but has no material impact on the controls within an ON device.

Table A.6

CSC	Title		Applicability to ON/OTNs
CSC 1	Inventory and Control of Enterprise Assets		Essential as pre-requisite for system analysis
	CSC1.1	Establish and Maintain Detailed Enterprise Asset Inventory	
	CSC1.2	Address Unauthorized Assets	
	CSC1.3	Utilize an Active Discovery Tool	Not applicable
	CSC1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	Not applicable
	CSC1.5	Use a Passive Asset Discovery Tool	Not applicable
CSC 2	Inventory and Control of Software Assets		As above where software is an asset
	CSC2.1	Establish and Maintain a Software Inventory	
	CSC2.2	Ensure Authorized Software is Currently Supported	Not applicable
	CSC2.3	Address Unauthorized Software	Not applicable
	CSC2.4	Utilize Automated Software Inventory Tools	Not applicable
	CSC2.5	Allowlist Authorized Software	
	CSC2.6	Allowlist Authorized Libraries	
	CSC2.7	Allowlist Authorized Scripts	
CSC 3	Data Protection		
	CSC3.1	Establish and Maintain a Data Management Process	Generally only applies at data source so out of scope of ON/OTNs other than by being part of the configuration data
	CSC3.2	Establish and Maintain a Data Inventory	As above
	CSC3.3	Configure Data Access Control Lists	Not in scope
	CSC3.4	Enforce Data Retention	Not in scope
	CSC3.5	Securely Dispose of Data	Not in scope
	CSC3.6	Encrypt Data on End-User Devices	End user devices are not in scope
	CSC3.7	Establish and Maintain a Data Classification Scheme	Not in scope as the ON/OTN should not have visibility of user level data classifications
	CSC3.8	Document Data Flows	Not in scope
	CSC3.9	Encrypt Data on Removable Media	Not in scope

CSC	Title		Applicability to ON/OTNs
	CSC3.10	Encrypt Sensitive Data in Transit	Whilst sensitive data is often only classifiable at the user level the provision of an encryption service is essential as an ON/OTN capability to be used by higher layer data services
	CSC3.11	Encrypt Sensitive Data at Rest	Not in scope (ON/OTNs only deal with moving data) (however see CSC4 for the case of management and configuration data) For keys and other critical configuration data and so on should be stored in a secure element (see clause 6.2.1)
	CSC3.12	Segment Data Processing and Storage Based on Sensitivity	Not in scope
	CSC3.13	Deploy a Data Loss Prevention Solution	Not in scope
	CSC3.14	Log Sensitive Data Access	In scope in the abstract and not especially in respect of data protection (See CSC13 for specific applicability to ON/OTN)
CSC 4	Secure Configuration of Enterprise Assets and Software		
	CSC4.1	Establish and Maintain a Secure Configuration Process	Directly applies (see clause 4.4 of the present document)
	CSC4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Directly applies (see clause 4.4 of the present document)
	CSC4.3	Configure Automatic Session Locking on Enterprise Assets	Not applicable. The network should rather be designed for 99,999 % availability. It may be reasonable to add this practice to NMS access but the counter risk of a malicious user forcing lockout should be considered
	CSC4.4	Implement and Manage a Firewall on Servers	Not applicable
	CSC4.5	Implement and Manage a Firewall on End-User Devices	Not applicable
	CSC4.6	Securely Manage Enterprise Assets and Software	Implements a specialization of CSC4.2
	CSC4.7	Manage Default Accounts on Enterprise Assets and Software	Not applicable - whilst there should be an administration account there should be no user level access accounts on network equipment
	CSC4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	Not applicable
	CSC4.9	Configure Trusted DNS Servers on Enterprise Assets	Not applicable (DNS lies at a higher layer than the ON/OTN)
	CSC4.10	Enforce Automatic Device Lockout on Portable End-User Devices	Not applicable
	CSC4.11	Enforce Remote Wipe Capability on Portable End-User Devices	Not applicable
	CSC4.12	Separate Enterprise Workspaces on Mobile End-User Devices	Not applicable
CSC 5	Account Management		Not directly applicable as CSC5 applies to the user and ONs do not have direct users (in the meaning of this CSC)
	CSC5.1	Establish and Maintain an Inventory of Accounts	
	CSC5.2	Use Unique Passwords	
	CSC5.3	Disable Dormant Accounts	
	CSC5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	
	CSC5.5	Establish and Maintain an Inventory of Service Accounts	A service account may be mapped to an account maintained at a device to allow management of the device. Thus CSC5.5 is closely aligned to CSC1.1
	CSC5.6	Centralize Account Management	As for CSC5.5 and CSC1.1

CSC	Title		Applicability to ON/OTNs
CSC 6	Access Control Management		
	CSC6.1	Establish an Access Granting Process	Not applicable
	CSC6.2	Establish an Access Revoking Process	Not applicable
	CSC6.3	Implement MFA for Externally-Exposed Applications	Not applicable
	CSC6.4	Implement MFA for Remote Network Access	Not applicable
	CSC6.5	Implement MFA for Administrative Access	Not applicable
	CSC6.6	Establish and Maintain an Inventory of Authentication and Authorization Systems	Not applicable
	CSC6.7	Centralize Access Control	Not applicable
	CSC6.8	Define and Maintain Role-Based Access Control	May be applicable but extended to ABAC
CSC 7	Continuous Vulnerability Management		
	CSC7.1	Establish and Maintain a Vulnerability Management Process	The controls of CSC7 apply for the entire network or system (not just the ON/OTN elements). The guidance given in ETSI TR 103 838 [i.41] applies.
	CSC7.2	Establish and Maintain a Remediation Process	
	CSC7.3	Perform Automated Operating System Patch Management	
	CSC7.4	Perform Automated Application Patch Management	
	CSC7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets	
	CSC7.6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	
	CSC7.7	Remediate Detected Vulnerabilities	
CSC 8	Audit Log Management		
	CSC8.1	Establish and Maintain an Audit Log Management Process	For the entire network (not just the ON/OTN elements)
	CSC8.2	Collect Audit Logs	
	CSC8.3	Ensure Adequate Audit Log Storage	
	CSC8.4	Standardize Time Synchronization	
	CSC8.5	Collect Detailed Audit Logs	
	CSC8.6	Collect DNS Query Audit Logs	
	CSC8.7	Collect URL Request Audit Logs	
	CSC8.8	Collect Command-Line Audit Logs	
	CSC8.9	Centralize Audit Logs	
	CSC8.10	Retain Audit Logs	
	CSC8.11	Conduct Audit Log Reviews	
	CSC8.12	Collect Service Provider Logs	
CSC 9	Email and Web Browser Protections		Not applicable to oNs
	CSC9.1	Ensure Use of Only Fully Supported Browsers and Email Clients	
	CSC9.2	Use DNS Filtering Services	
	CSC9.3	Maintain and Enforce Network-Based URL Filters	
	CSC9.4	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	
	CSC9.5	Implement DMARC	
	CSC9.6	Block Unnecessary File Types	
	CSC9.7	Deploy and Maintain Email Server Anti-Malware Protections	
CSC 10	Malware Defences		Not applicable specifically to ONs
	CSC10.1	Deploy and Maintain Anti-Malware Software	
	CSC10.2	Configure Automatic Anti-Malware Signature Updates	
	CSC10.3	Disable Autorun and Autoplay for Removable Media	
	CSC10.4	Configure Automatic Anti-Malware Scanning of Removable Media	
	CSC10.5	Enable Anti-Exploitation Features	
	CSC10.6	Centrally Manage Anti-Malware Software	

CSC	Title		Applicability to ON/OTNs
	CSC10.7	Use Behaviour-Based Anti-Malware Software	
CSC 11	Data Recovery		Not applicable to the ON in general although the processes apply for recovery of management and configuration data for which CSC4 directly applies
CSC 12	Network Infrastructure Management		
CSC 13	Network Monitoring and Defence		13.2 and 13.3 for NIDS in particular apply and will need further study for specific device types and configurations
CSC 14	Security Awareness and Skills Training		Not applicable
CSC 15	Service Provider Management		Not applicable
CSC 16	Application Software Security		Not applicable
CSC 17	Incidence Response Management		Not applicable
CSC 18	Penetration Testing		Not applicable

A.5 Specific risk analysis for ONs

A.5.1 Risks to confidentiality

NOTE: The metrics, and the tables, used in clause A.5 are taken from ETSI TS 102 165-1 [i.6].

The assumption is that all user and management traffic is carried between nodes on optical fibre and that data can be intercepted and copied from an optical fibre by a skilled operative.

Table A.7

Asset	Threat Category (CIA)	Threat	Description of attack	Attack analysis					Impact (resultant)	Risk
				Factor	Analyst estimation	Value	Potential	Likelihood		
Transferred data	Confidentiality	Interception	The attacker physically taps the fibre to copy content (raw bits)	Time	<= 1 day	0	Basic	Very likely	Medium	**Critical**
				Expertise	Proficient	3				
				Knowledge	Public	0				
				Opportunity	Easy	1				
				Equipment	Specialized	4				
				Attacker Theat level		Moderate				
				Attacker motivation	Medium (interested)					
				Attacker capability	Limited					
				Asset Impact	Medium	2				
				Resultant impact	Medium	2				
				Intensity	Single instance	0				

In the assessment the following criteria apply: The attacker needs specialized equipment to perform the attack (i.e. whilst the necessary tools are readily available they are not available other than in specialized outlets); An attacker needs to have a reasonable degree of proficiency to install a tap point without either being easily detected or destroying the communications ability of the cable. The impact is assessed to be medium resulting in an overall risk of critical.

As the likelihood of interception is "very likely" it is essential to minimize the impact. This can be achieved by encryption of traffic such that an attacker can recover no meaningful information from the intercepted data. Of itself encryption will only lower the risk to "Major". In order to bring the risk level to "Minor" additional methods of preventing the attacker from making the interception point are required. The intent in this case is to make the opportunity metric at least "difficult" and may include using passive and active measures to detect interference with the physical cable and devices on the cable, and any additional non-technical deterrents including taking legal (criminal) action against attackers. The result of applying each of these measures is shown below.

Table A.8

Asset	Threat Category (CIA)	Threat	Description of attack	Attack analysis					Impact (resultant)	Risk
				Factor	Analyst estimation	Value	Potential	Likelihood		
Transferred data	Confidentiality	Interception	The attacker physically taps the fibre to copy content (raw bits)	Time	<= 1 day	0	High	Unlikely	Low	**Minor**
				Expertise	Proficient	3				
				Knowledge	Public	0				
				Opportunity	Difficult	10				
				Equipment	Specialized	4				
				Attacker Theat level		Moderate				
				Attacker motivation	Medium (interested)					
				Attacker capability	Limited					
				Asset Impact	Low	1				
				Resultant impact	Low	1				
				Intensity	Single instance	0				

A.5.2 Risks to integrity

Integrity risks, resulting from manipulation of data in transit, when the transport of data is using optical means only, without store and forward elements in the optical path, are not possible without artificially intercepting and capturing traffic, modifying it, and then reinjecting the traffic. Assuming, as devil's advocate, that this was achievable and undetectable, it is assumed that the attack will be "targeted" in that the attacker is able to manipulate data to the net benefit of the attacker. If the nature of the attack is targeted the impact to the victim will be "high", whereas if the attack is not targeted the impact will likely be "low".

Table A.9

Asset	Threat Category (CIA)	Threat	Description of attack	Attack analysis					Impact (resultant)	Risk
				Factor	Analyst estimation	Value	Potential	Likelihood		
User data	Integrity	Data manipulation	The attacker modifies specific content of the data	Time	<= 2 months	7	Beyond High	Very unlikely	High	**Major**
				Expertise	Expert	6				
				Knowledge	Critical	11				
				Opportunity	Difficult	10				
				Equipment	Specialized	4				
				Attacker Threat level		Moderate				
				Attacker motivation	Medium (interested)					
				Attacker capability	Limited					
				Asset Impact	High	3				
				Resultant impact	High	3				
				Intensity	Single instance	0				

In addition to risks to integrity of data in transit the ON needs to take due account of other integrity attacks, in particular on system software of devices, including configuration data in the management plane. There are similar attacker problems when considered only at the optical layer, suggesting the risk is major (as impact is high).

NOTE: If the attacker can access data at a higher layer than the optical network the risk changes to critical as it is more straightforward to isolate data intended for a single user (access is given to IP addresses for example) thus likelihood changes to likely or worse. However the risk at higher layers is not specific to ON and not considered in detail in the present document.

A.5.3 Risks to availability

Availability risks are very broad in the definition from the CIA paradigm, however the ON is generally agnostic to many of the risks and attacks that directly address availability.

Annex B (informative): Stage 2 mapping to devices and equipment

B.1 Purpose of mapping exercise

In a conventional stage 2 document it is normal practice to identify mappings of Functional Elements and Reference Points to interfaces and devices. The primary purpose of these mappings is to drive the stage 3 specifications that follow on from the stage 2 definitions to have practical models for the combination of FEs and Reference Points into mapped device functions and interfaces.

NOTE: The device configurations given in this annex are indicative and do not impose requirements on any manufacturer to configure their devices in this manner.

B.2 Reference device model for Optical Transport Network and allocation of security functions to devices

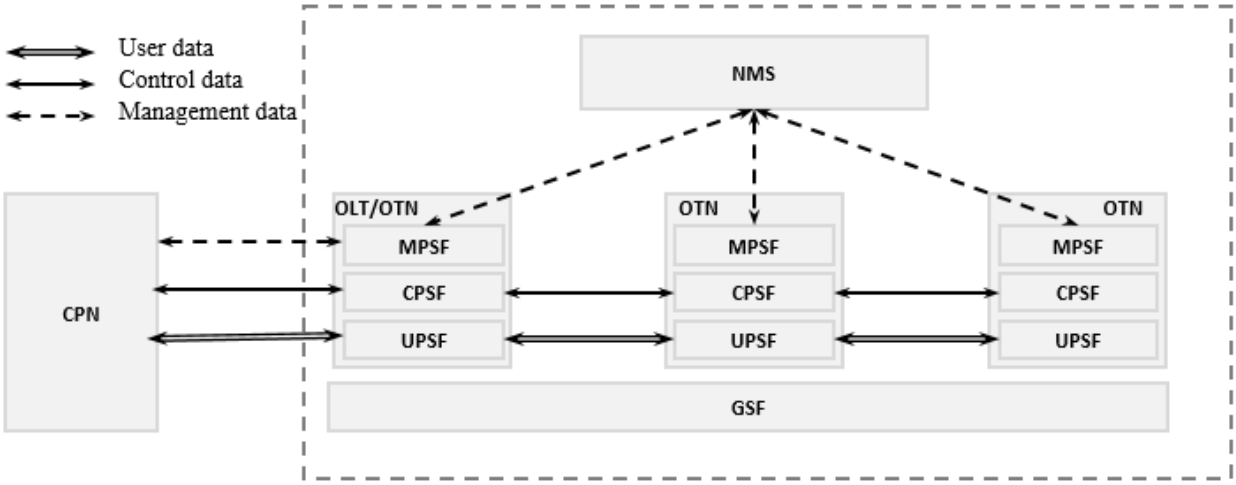

Figure B.1: Optical network architecture (functional level)

As shown in Figure B.1 the functional view of the optical network architecture includes OLT, OTN, NMS and their connections.

NOTE: The detailed security requirements for each of OLT, OTN and NMS will be extended through separate technical specifications based on present document.

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.

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

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

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

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

Annex C (informative): Assignment of trust domains and security associations for key management in OTNs

ETSI TR 102 419 [i.29] has summarized the role of Security Associations and the outline there is expanded as follows, and in the wider context of ETSI TS 102 165-2 [i.2], for the OTN case. *A Security Association (SA) is a relationship between two or more entities of the OTN that describes how the entities will utilize security services to communicate securely. This relationship is represented by a set of information that establish a security contract between the entities. The information (scope of the SA, policy elements of the SA, technical provisions of the SA) are mutually agreed by all the participating entities of the SA.* For the purposes of the present document the SA, consistent with the outline in ETSI TS 102 165-2 [i.2], identifies the following set of information between entities A and B:

$SA_{A,B}$ is a function of {ID_A, ID_B, CIA-capability, [Algorithm], [Key-size], [Key-management policy] …}

Where ID_A is the identity of end-point A of the link, ID_B is the identity of end-point B of the link.

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).

A detailed outline of trust is given in ETSI GR NFV-SEC 003 [i.24] and for the purposes of the present document the role of trust domain is similarly defined by administration and function. The definition of trust as "*confidence in the integrity of an entity for reliance on that entity to fulfil specific responsibilities*" and for the purpose of the present document this definition is equivalent to that of the SA extended to address trust in the policy that is identified in the SA.

The approach identified in the main body of the present document identifies a set of security operations across the ON that, when combined, result in a trusted link based on the trust associated to each security association. This model assures that ONs support the Zero Trust model outlined for Encrypted Traffic Integration in ETSI GR ETI 002 [i.12].

Annex D (informative): Cryptographic algorithm selection

Algorithms used in the context of ONs should have the following properties:

- Quantum safe, or quantum agile:
  - Whilst crypto-agility in general should be supported this capability should be extended to ensure that algorithms that are considered as quantum safe can be added to the device.
- Operate in a mode that does not allow error propagation to succeeding blocks.
- Able to operate in both block and streaming encryption mode.

EXAMPLE 1: For encryption AES256-CTR mode defined in FIPS 197 [i.18] (and equivalent ISO/IEC 18033-3 [i.42]) meets the above requirement assuming that the platform is responsible for meeting the crypto agility requirement.

In addition the criteria for hashing functions outlined in ETSI TS 102 165-2 [i.2] apply:

- One way function requirement
  - Given a hash h it should be difficult to find any message m such that $h = \text{hash}(m)$.
- Collision resistance requirement
  - Given an input $m1$ it should be difficult to find another input $m2$ such that $m1 \neq m2$ and $\text{hash}(m1) = \text{hash}(m2)$
- Strict Avalanche Criterion
  - if 1 bit in message m changes all other bits should change with 50 % probability
- Bit Independence Criterion
  - output bits j and k should change independently when any single input bit i is inverted, for all i, j and k

The algorithms used to generate a hash function should be of similar strength to any other cryptographic operation in the system but the system should ensure that it supports the concept of crypto agility in order that the algorithm can be updated over time.

EXAMPLE 2: For hashing SHA defined in FIPS 180-4 [i.19] applies.

EXAMPLE 3: For authentication the challenge response approach using hash functions as outlined in ETSI TS 102 165-2 [i.2] applies.

Annex E (informative): Bibliography

E.1 Articles on tapping of optical fibre

- Dominguez, Ismel, et al.: "Intrusive Passive Optical Tapping Device", IEEE™ Access 9 (2021): 31627-31637.
- M. Zafar Iqbal, H. Fathallah and N. Belhadj: "Optical fiber tapping: Methods and precautions," 8th International Conference on High-capacity Optical Networks and Emerging Technologies, 2011, pp. 164-168, doi: 10.1109/HONET.2011.6149809.
- J. Ph. Poizat and P. Grangier: "Experimental realization of a quantum optical tap", Phys. Rev. Lett. 70, 271 - Published 18 January 1993.

E.2 Cross referenced ISO documents

- ISO/IEC 20543: "Information technology - Security techniques - Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408".
- ISO/IEC 19790:2012: "Information technology - Security techniques - Security requirements for cryptographic modules".
- ISO 7498-2: "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture".

NOTE: ISO 7498-2 and Recommendation ITU-T X.800 [i.14] contain the same text.

E.3 Regulatory documents

- Cyber Security Act (CSA): "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)".
- Cyber Resilience Act (Draft text from September 2022): "Proposal for a Regulation on cybersecurity requirements for products with digital elements - Cyber resilience Act".
- NIS2: "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".
- Radio Equipment Directive (RED): "Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC".
- General Data Protection Directive (GDPR): "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)".

History

Document history		
V1.1.1	December 2022	Publication