ETSI GS F5G 012 V1.1.1 (2023-01)

Fifth Generation Fixed Network (F5G); Security; F5G Security Countermeasure Framework Specification

Disclaimer

The present document has been produced and approved by the Fifth Generation Fixed Network (F5G) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGS/F5G-0012 Security

Keywords
artificial intelligence, cyber security, F5G, security, security by default

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 4
Foreword 4
Modal verbs terminology 4
1 Scope 5
2 References 5
2.1 Normative references 5
2.2 Informative references 5
3 Definition of terms, symbols and abbreviations 6
3.1 Terms 6
3.2 Symbols 7
3.3 Abbreviations 7
4 Introduction and review of threats to F5G 8
5 Security requirement and features 10
5.1 Overview 10
5.2 UP.UD.001, tapping of cable 12
5.2.1 Re-assessment of risk and likelihood 12
5.2.2 Confidentiality and integrity protection of content 12
5.2.3 Detection of a tap point 12
5.3 UP.UD.002, data modification at source 13
5.4 UP.NE.001 and UP.NE.002, access to data on network elements 13
5.5 UP.NE.003, UP.NE.004 modification of system software and firmware 14
5.6 UP.NE.005, denial of service (physical attack) 14
5.7 UP.NE.006, denial of service (packet flooding) 14
6 F5G specific application of mitigations 15
6.1 Establishment of security architecture 15
6.2 Network management domain security requirements 16
6.3 Network transport domain security requirements 16
6.4 Network domain security requirements 16
6.4.1 Security associations in F5G 16
6.4.2 Entity identification in F5G 17
Annex A (normative): Quantum safe cryptographic provisions 18
Annex B (informative): The role of trust in security assurance 19
B.1 Trust as a synonym for security 19
B.2 Scope of trust 19
B.3 Models of trust 20
B.4 Evaluation or testing of trust 21
B.5 Invalidating trust 21
B.6 Development of a trust manager 21
Annex C (informative): Bibliography 23
C.1 ETSI documents in development at time of publication 23
C.2 Data encoding and error correction schemes 23
C.3 Other security documents 23
History 24

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 Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Fifth Generation Fixed Network (F5G).

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 specifies security countermeasures against security threats to F5G as defined by its purpose [i.15] and use cases (ETSI GR F5G 008 [i.1]), its architecture (ETSI GS F5G 004 [i.2]) and informed by the Risk Analysis in ETSI GR F5G 010 [i.3].

The identified measures in the present document are those achievable by technical means. In addition the present document identifies, but does not fully specify, mitigations that require non-technical measures.

2 References

2.1 Normative references

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

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

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 103 924: "Optical Network and Device Security Catalogue of requirements".

[2] ETSI TS 102 165-2: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures".

2.2 Informative references

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

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

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

[i.1] ETSI GR F5G 008: "Fifth Generation Fixed Network (F5G); F5G Use Cases Release #2".

[i.2] ETSI GS F5G 004: "Fifth Generation Fixed Network (F5G); F5G Network Architecture".

[i.3] ETSI GR F5G 010: "Fifth Generation Fixed Network (F5G); Security; Threat Vulnerability Risk Analysis and countermeasure recommendations for F5G".

[i.4] NIST Cybersecurity Framework, the Five Functions.

NOTE: Available at https://www.nist.gov/cyberframework/online-learning/five-functions.

[i.5] Recommendation ITU-T X.800: "Security Architecture for Open Systems Interconnection for CCITT Applications".

[i.6] 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 contain the same text.

[i.7] ETSI EG 203 310: "CYBER; Quantum Computing Impact on security of ICT Systems; Recommendations on Business Continuity and Algorithm Selection".

[i.8] Recommendation ITU-T G.873.2: "Digital networks - Optical transport networks: ODUk shared ring protection".

[i.9] Recommendation ITU-T G.873.3: "Digital networks - Optical transport networks: Optical transport network - Shared mesh protection".

[i.10] ISO/IEC 14763-2:2019: "Information technology -- Implementation and operation of customer premises cabling -- Part 2: Planning and installation".

[i.11] ISO/IEC 14763-3:2014: "Information technology -- Implementation and operation of customer premises cabling -- Part 3: Testing of optical fibre cabling".

[i.12] ETSI EN 303 645: "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

[i.13] NIST SP 800-155 (draft): "BIOS Integrity Measurement Guidelines".

[i.14] ETSI GS NFV-SEC 003: "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance".

[i.15] Terms of Reference of ETSI ISG F5G.

NOTE: Available from https://portal.etsi.org/Portals/0/TBpages/F5G/ISG_F5G_ToR_D-G_APPROVED_20211203.pdf.

[i.16] ETSI GS F5G 006 (V1.1.1): "Fifth Generation Fixed Network (F5G); End-to-End Management and Control; Release #1".

[i.17] ETSI TS 103 486: "CYBER; Identity Management and Discovery for IoT".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

crypto-agile: able to change or replace the existing suite of cryptographic algorithms or parameters with ease and without the rest of the F5G infrastructure being significantly affected

delegated trust: trust arising where an entity A is unable to evaluate the appropriate level of trust for a relationship with another entity B, A chooses to delegate the decision to another entity C, which is in a better position to make such a decision

NOTE 1: For delegated trust there is a precondition that there is a direct trust relationship from entity A to entity C.

NOTE 2: In this form of delegated trust entity C is aware of the relationship between entity A and entity B.

direct trust: trust decision by an entity A to trust entity B without any other party being involved

transitive trust: trust decision by an entity A to trust entity B because entity C trusts it

NOTE: Transitive trust differs from simple delegated trust (see above) as entity C does not know of the relationship between entity A and entity B.

trust domain: collection of entities between which there is either direct, delegated or transitive trust in the authenticity of identifiers and the respecting of privacy requirements that share a set of security policies that mitigate any risk of exploit to the grouping and/or collection within the trust domain boundary

3.2 Symbols

Void.

3.3 Abbreviations

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

AAT	Authority Attribute Tree
ABAC	Attribute Based Access Control
ABC	Attribute Based Cryptography
AES	Advanced Encryption System
AggN	Aggregation (of N connections)
AI	Artificial Intelligence
AU	AUthentication
CIA	Confidentiality Integrity Availability
CPE	Customer Premises Equipment
CPN	Customer Premises Network
CRC	Cyclic Redundancy Code
CSP	Communications Service Provider
CTR	Counter
DC	Data Centre
DC-GW	Data Centre Gateway
DCH	Dedicated Transport Channel
DoS	Denial of Service
DTS	Draft Technical Standard/Specification
E2E	End to End
EC	Exchange Carrier
ECDSA	Elliptic Curve Digital Signature Algorithm
ETH	Ethernet
EVPN	Ethernet Virtual Private Network
FTTR	Fibre To The Room
GCM	Galois Counter Mode
HSM	Hardware Security Module
ICT	Information Communications Technology
IdM	Identity Management
IP	Internet Protocol
LDC	Local Data Centre
M&C	Management and Control
MCA	Management, Control and Analytics
NIST	National Institute of Standards and Technology
NTRU	N^{th} degree Truncated polynomial Ring Units
ODU	Optical Data Unit
OLT	Optical Line Terminal
OSI	Open Systems Interconnection
OSU	Optical Service Unit
OTDR	Optical Time Domain Reflectometry
OTN	Optical Transport Network
OTNF	OTN Fabric
P2P	Peer to Peer
pBNG	physical Broadband Network Gateway
PE	Provider Edge
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
RoT	Root of Trust
RS	Reed Solomon

RSA	Rivest-Shamir-Adleman
RTM	Root of Trust for Measurement
RTR	Root of Trust for Reporting
RTS	Root of Trust for Storage
SA	Security Association
SAP	Service Access Pont
SMP	Service Mapping Point
SP	Service Point
SPP	Service Processing Point
TV	Television
VLAN	Virtual Local Area Network
VXLAN	Virtual eXtensible Local Area Network
ZTA	Zero Trust Architecture

4 Introduction and review of threats to F5G

In ETSI GR F5G 010 [i.3], table 6.6-1 a simplified threat analysis of F5G summarized the threats specific to the optical nature of the Underlay Plane and identified a number of countermeasures as in table 4.1. The present document addresses the capabilities identified in [i.3], and also addresses considerations to be made for data assurance and resilience arising from applicable regulation. Topics on the F5G Service Plane is for further study.

Table 4.1: Mitigations against quantified risk assessments (partial from ETSI GR F5G 010 [i.3])

Threat	Risk	Recommended countermeasures
UP.UD.001, tapping of cable	Major	Data encryption and detection of the existence of tap devices
UP.UD.002, data modification at source	Major	Integrity proof and verification of data content
UP.NE.001, access to data on device	Major	Access control (including aspects of identity management) and intruder detection systems
UP.NE.002, access to data on device	Critical	Access control (including aspects of identity management) and intruder detection systems. System integrity mechanisms to detect changes in software
UP.NE.003, modification of system firm ware	Critical	System integrity mechanisms to detect changes in software. Secure boot (may include remote attestation of system images)
UP.NE.004, modification of system software with malicious code	Critical	System integrity mechanisms to detect changes in software. Secure boot (may include remote attestation of system images)
UP.NE.005, denial of service (physical attack)	Critical	Redundancy protection (e.g. measures in Recommendations ITU-T G.873.2 [i.8], G.873.3 [i.9]). In addition, the measures identified in clauses 5.6 and 5.7 apply (see note 2).
UP.NE.006, denial of service (packet flooding)	Critical	Management plane and service plane coordinated traffic analysis and throttling or redirection measures
SP.AS.3, denial of service (attack at the service plane to initiate denial of service)	Major	Management plane and service plane coordinated traffic analysis and throttling or redirection measures
MCAP.MC.1, interception	Major	Access control and encryption of management plane and control data
MCAP.MC.2, confidentiality (unauthorized access)	Major	Access control and encryption of management plane and control data
MCAP.MC.3, integrity	Major	Timestamp and provide integrity proof mechanism against an adversary seeking to manipulate data (e.g. use digitally signed content between management controllers and managed entities)
MCAP.MC.4, availability	Major	To prevent the attacker disabling the configuration channels between network element and NMS access to these channels shall be restricted to authenticated and authorised elements only
NOTE 1: Only those risks considered as major or critical from ETSI GR F5G 010 [i.3] are addressed in detail in the present document. NOTE 2: Measures to protect against physical attack are not defined in the present document and have been addressed in part in ETSI GR F5G 010 [i.3].		

The present document further develops the countermeasures identified in table 4.1 in the form of a security framework, with the exception of countermeasures for physical attack (UP.NE.005) where non-ICT or non-technical measures apply.

Each countermeasure is identified with respect to the security association it represents. More than one security association may exist between any pair of Principal and Relying Party. The security association stakeholders are:

- Principal - the entity making an assertion of one of the Confidentiality/Integrity/Availability CIA attributes.
- Relying Party - the entity that requires to act on data from the Principal and that has to build trust in the capability of the Principal to deliver data within the security association.
- Association Authority - the entity that acts as an independent 3rd party to support the attestations made by the Principal.

In general, countermeasures are developed with a model of Identify, Protect, Detect, Respond, and Recover (see [i.4] and the figure "The NIST framework principles" in it) with some exceptions for anticipatory attack based on the outcome of the risk analysis.

EXAMPLE: The risk analysis of ETSI GR F5G 010 [i.3] identified tapping of an optical fibre to be a major risk, as the likelihood is modelled as significant and the cost of provision of the countermeasure is relatively low as a pre-emptive measure, but high to be implemented after the system has gone operational. It may also be the case that the tapping of the fibre and eavesdropping of data is/were not detected, even over a long time, but the consequences of user data disclosure cannot be quantified.

In architectural modelling for security measures the layered model of Recommendation ITU-T X.800 [i.5] is adopted in the present document. In this model Layer-N offers a service to Layer-N+1. In many applications of the OSI security model Layer-N+1 "manages" the security association of Layer-N, most often this is as part of an explicit strategy to bind Layer-N to Layer-N+1, for example, by authentication processes at layer 3 deriving an encryption key for use at layer 2.

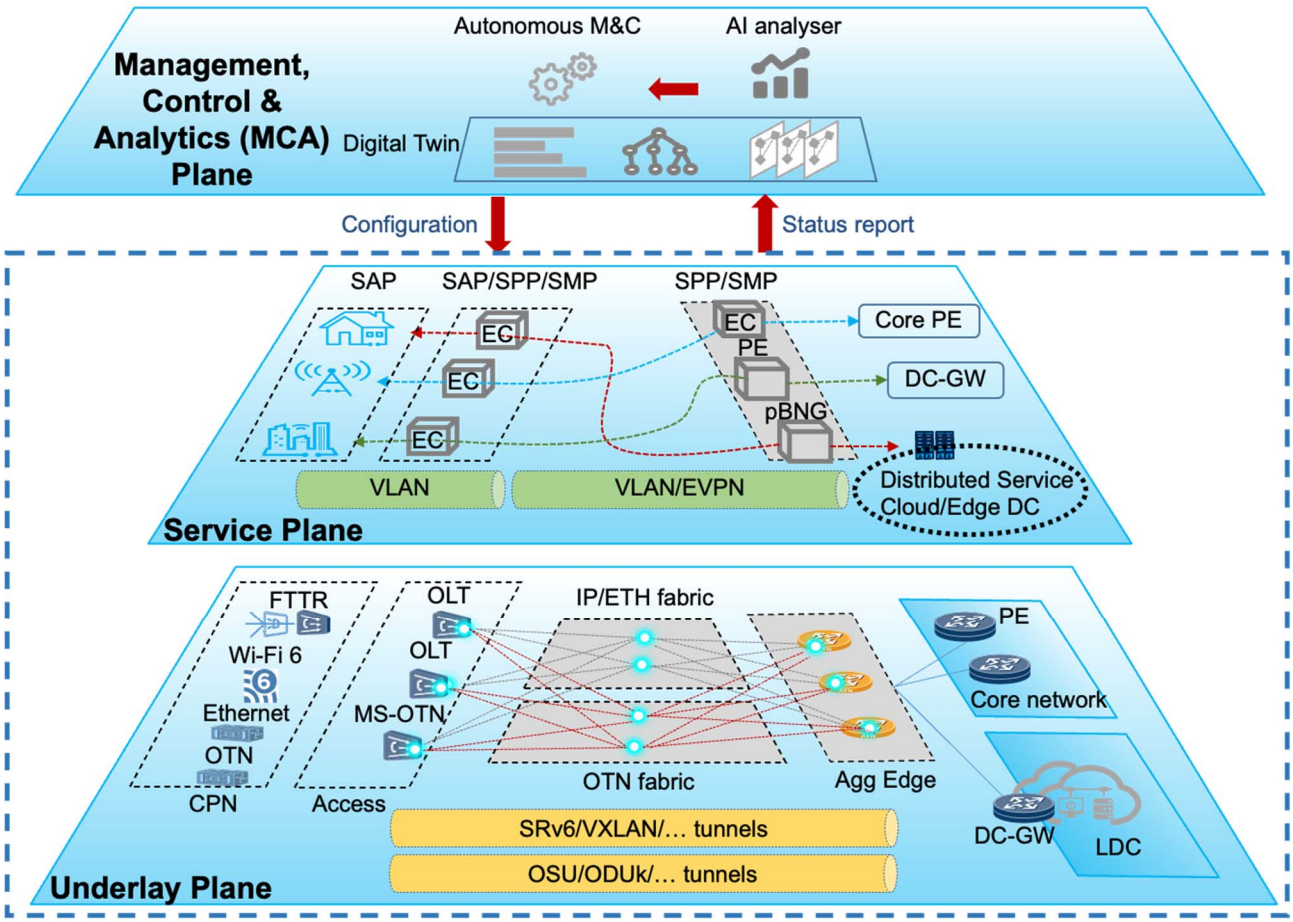

Figure 4.1: F5G network architecture from ETSI GS F5G 004 [i.2]

The F5G network (see figure 4.1) architecture is comprised of 3 planes, an Underlay Plane, a Service Plane and a Management, Control & Analysis Plane (MCA Plane). The information hiding model from OSI (defined in Recommendation ITU-T X.800 [i.5] and in ISO 7498-2 [i.6]) also applies to the planar architecture model.

One of the purposes of the MCA plane is to maximize performance of the Service and Underlay planes. The data collected (push and pull) by the MCA plane functionality should be used to assist in the detection and identification of security violations and to dynamically adapt measures if necessary (for example, this could apply to DoS detection and to detection of botnets). For a more detailed management architecture refer to ETSI GS F5G 006 [i.16].

5 Security requirement and features

5.1 Overview

The countermeasures identified in the present document expand on the major and critical risks identified in ETSI GR F5G 010 [i.3] as shown in table 4.1 of the present document. Taken overall where network elements (software or hardware) and services operate dynamically and where the principle of security by default applies to F5G and mapping to the obligations arising from regulation the following principles have been taken into account in the high level approach to security provisions in F5G:

- Make "security by default" an active choice
  - Verify every claim (in the CIA paradigm) of every element in the F5G system
- Verify every aspect of every security-connection that has potential to be malicious

NOTE 1: Any publicly operated network has to meet a number of regulatory obligations to protect users and dependent entities. Whilst many such obligations place security constraints directly on the network through the operator (as the liable party) the provisions in the present document are not offered in direct response to any such regulation but provide the highest reasonable level of protection in an observable and explicable manner.

The conventional OSI security model shall apply with the extensions identified in table 5.1. Each active network element in the F5G network shall be able to identify itself and establish a set of security associations with each other entity it has to connect to in support of providing a service. Active network elements shall identify themselves semantically (i.e. by attestation of their F5G function) and contextually (e.g. by their physical or logical location) in addition to identification by provision of a canonical globally unique identifier. The functions of the OSI security (see Recommendation ITU-T X.800 [i.5]/ISO 7498-2 [i.6]) model apply as shown in table 5.1.

NOTE 2: Multiple F5G active network elements may share a semantic/functional identity and may therefore be distinguished by additional contextual attributes.

NOTE 3: Multiple schemes exist for semantic information but the specific scheme for F5G is not defined in the present document and is for further study.

Table 5.1: Review of OSI security service applicability to F5G

Layer	OSI security services	F5G specificity
7	Peer Entity Authentication; Data Origin Authentication; etc.	Provision of Trust manager in MCA plane linked to a hardware enabled root of trust. In particular this applies to the management interfaces as defined in ETSI GS F5G 006 [i.16].
6	Facilities provided by the presentation layer offer support to the provision of security services by the application layer to the application process. The facilities provided by the presentation layer rely on mechanisms which can only operate on a transfer syntax encoding of data. Security mechanisms in the presentation layer operate as the final stage of transformation to the transfer syntax on transmission, and as the initial stage of the transformation process on receipt	
5	No security services are provided in the session layer	
4	Peer Entity Authentication; Data Origin Authentication; Access Control service; Connection Confidentiality; Connectionless Confidentiality; Connection Integrity with Recovery; Connection Integrity without Recovery; and Connectionless Integrity	
3	Peer entity authentication, Data origin authentication, Access control service, Connection confidentiality, Connectionless confidentiality, Traffic flow confidentiality, Connection integrity without recovery, Connectionless integrity	Applies primarily in the Underlay Plane. Links to a hardware enabled root of trust The application to the Service Plane is for further study, specifically for E2E layer 3 services.
2	Connection confidentiality, Connectionless confidentiality	
1	Connection confidentiality, Traffic flow confidentiality	Provision of a hardware root of trust.

In all cases each F5G physical network element shall have a hardware enabled root of trust (e.g. a Hardware Security Module (HSM)) acting as the root of trust for each of measurement, storage and reporting as outlined in clause 6. In addition the general principles outlined in ETSI EN 303 645 [i.12] apply as shown in table 5.2.

Table 5.2: Applicability of provisions of ETSI EN 303 645 [i.12] to F5G security

ETSI EN 303 645 general provision	F5G interpretation and applicability
No universal default passwords	F5G network elements are unlikely to use passwords hence this provision is extended to apply to identification and authentication credentials which shall follow the general constraints of being unique within the managed domain.
Implement a means to manage reports of vulnerabilities	Applies in full to F5G with reporting from the management plane to an operator.
Keep software updated	Applies in full to F5G (for all software types).
Securely store sensitive security parameters	Applies in full to F5G (see clause 6).
Communicate securely	Applies in full to F5G for all relevant connections.
Minimize exposed attack surfaces	Applies in full to F5G.
Ensure software integrity	Applies in full to F5G.
Ensure that personal data is secure (from the customer or related to any legal entity and given to F5G)	Applies in full to F5G.
Make systems resilient to outages	Applies to F5G in collaboration with the reporting of vulnerabilities
Examine system telemetry data	Applies in full to F5G.
Make it easy for users to delete user data	Applies where an F5G system directly or indirectly retains user identifiable data (e.g. usage logs).
Make installation and maintenance of network elements easy	The F5G system should not impede system security by over complex maintenance and installation schemes. Applies from management plane to all managed entities.
Validate input data	Applies in full to F5G.

5.2 UP.UD.001, tapping of cable

5.2.1 Re-assessment of risk and likelihood

A "cable tap" is used by an adversary to intercept the content of communication. As identified in more detail in ETSI TS 103 924 [1] the likelihood of installation of a tap varies in complexity depending on where the fibre is tapped. It is strongly assumed that placing a tap at the network end is more difficult than at the customer end, although in both cases there is a strong likelihood of the attacker being stopped before successful implementation/installation of the tap.

In general, it is assumed that countermeasures requiring a decision (or some form of affirmative action) shall take place at a higher layer where the data required to inform the decision shall come from the lower layer.

EXAMPLE: The Underlay Plane acts as a measuring and data source for decisions made in the Service Plane or the MCA plane, and the Service Plane acts as measuring point and data source for decisions made in the MCA plane.

5.2.2 Confidentiality and integrity protection of content

As identified in ETSI GR F5G 010 [i.3] the suite of countermeasures includes data encryption that limits the harm caused when data is intercepted. The risk calculation from [i.3] suggest a Major risk with many physical mechanisms that can be applied to limit the physical tap being deployed, although it is reasonable to assume that any purely physical measure can be countered hence higher level mechanisms acting directly on the payloads (user and system data) shall be deployed (i.e. confidentiality and integrity protection applied above the physical layer (see also table 5.1)).

NOTE: Eavesdropping and interception are nearly synonyms. An interception may lead to eavesdropping. The difference in the context of the present document is that the signal is not broadcast and there is no "spillage" of signal to be eavesdropped thus in order to eavesdrop on the content of the fibre it has to be actively intercepted.

The mechanisms defined in ETSI TS 103 924 [1] shall apply to give confidentially protection to the optical payload in the network with the refinements identified in clauses 6.2 and 6.3 of the present document.

5.2.3 Detection of a tap point

As identified in ETSI GR F5G 010 [i.3] the suite of countermeasures includes the detection of the existence of tap devices.

Characteristics of an optical tap that can be used in detection:

- A physical discontinuity as a result of the bend in the fibre made by the attacker (i.e. the fibre and its casing will be physically compromised).
- Change in expected link attenuation at time of insertion of the tap (i.e. there will be an increase in attenuation after the tap being inserted).

NOTE 1: Any expected link attenuation changes should be observable. A fibre of fixed length with a fixed intensity light source will have a predictable attenuation over the length of the cable (say 1,5 dB/km) that may be negatively impacted by the presence of a tap.

Edge nodes in the Underlay Plane maintain a record of the received signal strength at the CPE end of the fibre connection and at a point inside the Communications Service Provider's (CSP) domain of control. Any drop in received signal strength should initially be assumed to be an adversarial attack. If a node determines that there is a pattern of change of received signal strength consistent with a tap being inserted the attack pattern and location and shall be notified to the MCA plane and in some cases affected customers should be notified of a line fault. Each measurement should be attested to by the measuring entity identifying itself as authorized to make such a measurement by a recognized authority and the measurement should be signed in a manner that allows the recipient to verify the integrity of the measurement and the source of the measurement.

NOTE 2: The means by which attenuation increase is determined is not in the scope of the present document but may be achieved by recording any changes in the received light level but care should be taken to ensure that such detectors do not unnecessarily attenuate the signal. The sensitivity of the optical layer supervision detector should be sufficient to detect the presence of a tap (e.g. if the detector is only sensitive to (say) 3 dB but the tap only introduces a 0,5 dB attenuation the tap may not be detected).

The location of the optical tap unit may be determined using Optical Time Domain Reflectometry (OTDR) and physical resources should be dispatched to remove the unit and to repair the fibre.

EXAMPLE: If a tap device is identified at a known location a technician should remove the tap device from that location.

NOTE 3: Whilst OTDR is a well known means to identify optical line faults it is not fully standardized. The provisions of ISO/IEC 14763-3 [i.11] apply in part.

NOTE 4: Whilst OTDR can identify direct problems in the optical fibre, the determination of an attack may be achieved in other ways, such as observation of exceptional changes of resistivity or similar of the cable casing, although an attack on the casing does not imply that the optical content is intercepted.

5.3 UP.UD.002, data modification at source

As identified in ETSI GR F5G 010 [i.3] the suite of countermeasures should include proof (at source) and verification of the integrity of data content (at sink).

EXAMPLE: The source is associated to the data and if the data is modified that association remains so it will appear to be modified by the source. The intent of integrity measures is to ensure that what is sent by the source is what is received by the sink.

The mechanisms defined in ETSI TS 103 924 [1] shall apply to protect the integrity of the optical payload in the network.

A digital signature mode should be applied to data to provide the following security services (see also clause 6):

- Source and destination authentication.
- Confidentiality of data content.
- Proof of integrity of data content.

The general mechanisms for protection against threats of manipulation shall extend the mechanisms for software integrity (see clause 6) and shall be managed using Roots of Trust, as outlined in NIST SP 800-155 (draft) [i.13]. See also clause 6.

NOTE: Whilst the reference to NIST SP 800-155 is labelled as "draft" the content is publicly available and cited. The labelling of the document as draft does not infer that the content is unstable.

5.4 UP.NE.001 and UP.NE.002, access to data on network elements

As identified in ETSI GR F5G 010 [i.3] the suite of countermeasures should include the provisions of access control and intruder detection systems, with the addition of mechanisms to detect changes in software (see clause 5.5).

NOTE: An access control system can be parameterized in multiple ways to allow for a number of restrictions based on such things as identity of the accessing network element, the location of the accessing device, the time of day and so forth. The combination of capabilities suggests that a policy based, attribute access control system is to be preferred that operates across multiple planes.

Access control mechanisms are addressed in ETSI TS 102 165-2 [2] and shall be applied with successful authentication of any party accessing data as a pre-requisite of any access control policy. Mechanisms consistent with the models of Attribute Based Cryptography (ABC) for Attribute Based Access Control (ABAC) should be applied to ensure that personal data is not required for data access in core network elements.

5.5 UP.NE.003, UP.NE.004 modification of system software and firmware

As identified in ETSI GR F5G 010 [i.3] the suite of countermeasures should include the provision of system integrity mechanisms to detect changes in software, for example to ensure that the boot mechanism is not compromised wherever the system has to restart.

In particular on initial installation the system shall record the hash of the system firmware and store it in a Root of Trust for Storage (RTS). On each subsequent use the Root of Trust for Measurement (RTM) shall compare the hash of the current claimed firmware and compare it to the value from the RTS. If the values (stored and measured) are identical the system shall assert that the current firmware is unmodified.

NOTE: The term software is used as a shorthand for the many forms of code written for systems and executed on a processor. The degree of mutability, and the conditions of mutability, of software inform a number of variations of the term (e.g. firmware).

A network element shall only install software from a known and authorized source.

5.6 UP.NE.005, denial of service (physical attack)

As identified in ETSI GR F5G 010 [i.3] the suite of countermeasures should include the provision of measures that provide redundancy as a mode (or form) of protection, and which also limit the likelihood of an attacker gaining access to installations in order to physically harm the network or to disturb, interrupt or tamper with network functions.

NOTE: The use of redundancy provisions to be able to bypass system blocks may not be possible at the edge of the network and alternative provisions may need to be offered if a CPE is exposed to attacks.

Resilience measures as defined in Recommendations ITU-T G.873.2 [i.8], G.873.3 [i.9] should be applied, in addition to good building and installation practice as defined in ISO/IEC 14763-2 [i.10] and ISO/IEC 14763-3 [i.11].

5.7 UP.NE.006, denial of service (packet flooding)

As identified in ETSI GR F5G 010 [i.3] the suite of countermeasures should include the provision of measures that enable coordinated analysis of traffic transmitting intra and inter plane, as well as end-to-end, within the managed domain, to enable both, identification of a denial of service attack and to provide throttling of the source of the attack, or redirection of the target to mitigate attacks on the intended target.

NOTE: Not all F5G networks are packet based so provisions for prevention of packet flooding do not apply for those network types.

As indicated in clause 5.2.1 the Underlay Plane should act as a measuring and data source for decisions that are subsequently acted upon in the MCA. The algorithm to determine if a specific node is subject to a packet flooding is not defined in the present document, however the following should be considered in determination of a packet flooding attack (mainly applies in P2P scenarios given below):

- Requested data services from CPE and estimated data load.

EXAMPLE 1: A CPE would normally be expected to fall into a download volume range per unit time, within a normal diurnal cycle, consistent to the CPE type. This should act as the base line for determination of exceptional behaviour.

- Variation from accepted normal behaviour at CPE.
- Knowledge of exceptional events that may account for local CPE variations.

EXAMPLE 2: Sudden or prolonged increases in the load placed on the network by a CPE/ONU may be affected by external factors such as Working From Home, change of broadcaster patterns (e.g. move from terrestrial TV transmissions to Internet based TV).

Estimations of changes in CPE behaviour should not incur a change in the collection of personal or other traffic usage data from the CPE and wherever data is collected and collated against previous behaviour it shall be only processed in accordance with any regulatory obligations.

6 F5G specific application of mitigations

6.1 Establishment of security architecture

The security architecture overlays and extends the core connectivity architecture shown in figure 4.1. Each plane shall define a set of security authorities for each of authentication and authorization, as follows:

- Trust manager
- Authentication Authority
- Authorization Authority

As stated in ETSI GR F5G 010 [i.3] within the F5G architecture, trust should be constrained within each plane, and only for very specific relationships between planes. Thus each of the underplay plane, the service plane and the management plane should represent a single trust domain (see also Annex B). A trust manager, or root of trust should exist within each plane from which both transitive trust and delegated trust relationships can be assured. This shall enable the establishment of a trusted network.

Network element software integrity shall be managed using Roots of Trust (RoT), as outlined in NIST SP 800-155 (draft) [i.13], and used to support a model of transitive trust intra- (i.e. for entities within a single plane) and inter-plane (i.e. for entities in different planes, which is typically to and from the MCA plane). The following Roots of Trust shall be defined and implemented in the F5G system:

- RoT for Measurement (RTM)
  - The entity responsible to make reliable integrity measurements. It is the root of the chain of transitive trust for subsequent Measurement Agents.

NOTE: A small RTM applied very soon after a re-initialization of an endpoint may have greater value than an RTM instantiated later, mainly in minimizing the attack surface's exposure to subversion of the measurement process. The later the endpoint invokes the RTM, the more opportunity an adversary has to subvert the measurement trust chain. The larger the RTM, the greater the chance that a flaw in its implementation will provide an opportunity for an adversary to subvert the RTM.

- RoT for Storage (RTS)
  - The RTS shall maintain a tamper-evident summary of integrity measurement values and the sequence of those measurements, and shall hold integrity hashes for those sequences. These integrity hashes can either be used to verify the integrity of a log containing the integrity measurement values and the sequence of those measurements, or it can be used as a proxy for that log. The RTS maintains these integrity hashes in tamper-evident locations.
- RoT for Reporting (RTR)
  - The RTR shall enable reliable reporting information that is provided by the RTM and its Measurement Agent(s) or held by the RTS. The RTR serves as the basis for the capabilities of integrity and non-repudiation of reports of measurement data. It necessarily leverages the RTM and RTS. A key requirement for the RTR is an unambiguous identity, both of the endpoint and the components being measured and reported. This identity may be persistent or temporary. Signatures of measurement report data using keys are a common mechanism to provide unambiguous identity. Certificates for keys may certify membership in a group or identify a particular member.

6.2 Network management domain security requirements

Pending publication of specifications listed in annex C, bibliography which should be applied to F5G the following text summarizes the provisions expected from the listed specifications.

- The MCA plane shall act as the overall root of trust for the relevant operator and shall establish the trust domain of the operator.
- Entities in the Service Plane shall be integrated to the trust domain by proof of identity and proof of attestation of function to the MCA plane.
- The link between the Service Plane and the MCA plane is visible through the reporting and configuration interface (see figure 4.1) and the interface shall be within the trust domain.

NOTE: The format of the interface is independent of the necessary trust to be established across it.

- The MCA plane shall maintain the security policy for the trust domain.

The provisions of the TC CYBER-Specialisation of ETSI TS 103 924 [1] for provisions in the management of Optical Network elements and services (see annex C, bibliography) should apply in due course.

6.3 Network transport domain security requirements

Pending publication of specifications listed in annex C, bibliography which should be applied to F5G the following text summarizes the provisions expected from the listed specifications.

- All entities in the Underlay plane shall be identified to each other and shall join the trust domain established by the MCA plane.
- Connections wholly within the underlay plane shall be within the trust domain established by the MCA plane and shall also comply to the security policy of the trust domain.
- The security policy relevant to the underlay plane should enforce link encryption and link integrity verification.
- The security policy relevant to the underlay plane should also enforce multi-link payload encryption and integrity verification.

The provisions of CYBER-Specialisation of ETSI TS 103 924 [1] for provisions in access network elements (see annex C, bibliography) should apply in due course.

The provisions of CYBER-Specialisation of ETSI TS 103 924 [1] for provisions in transport network elements (see annex C, bibliography) should apply in due course.

6.4 Network domain security requirements

6.4.1 Security associations in F5G

In addition to the provisions of cited above the following apply.

The following Security Associations (SAs) shall be defined.

Table 6.1: Identification of security associations

SA-ref (see notes)	Initiating network entity	Terminating network entity	SA type	SA enforcement mechanism
SA-CPE-OA-AU	CPE/CPN/ONU	OLT/MS-OTN (comprising the Optical Access elements of figure 4.1)	Authentication	AAT attestation
SA-OLT-OTNF-AU	OLT	OTN fabric (OTN-based AggN)	Authentication	AAT attestation
SA-OLT-OTN-INT	OLT	OTN fabric (OTN-based AggN)	Integrity	AAT attestation
SA-OF-AE-AU	OTN fabric (OTN-based AggN Edge Node)	Aggregation Edge	Authentication	
SA-CPE-OA-CFD	CPE/ONU	Access Node	Confidentiality	Signed and encrypted data
SA-CPE-OA-INT	CPE/ONU	Access Node	Integrity	Signed and encrypted data
NOTE 1: The SAs are named with reference to the initiating entity, the terminating entity, and the form of CIA attribute, thus SA-CPE-OA-AU initiates at the CPE, terminates in the Access Node shown in figure 4.1 and is of type authentication. NOTE 2: Additional SAs may be added by implementation of capabilities arising from clauses 6.2 and 6.3.				

6.4.2 Entity identification in F5G

The general approach to entity and capability identification outlined in ETSI TS 103 486 [i.17] should apply to F5G in support of the ZTA model. An F5G entity performing an identifiable function shall be able assert to that function as an attribute of the entity (i.e. it shall be attested to as an attribute of the entity using the methods defined in [i.17]). Each SA (see clause 6.4.1) shall verify the assertion of each attribute it links to.

Annex A (normative): Quantum safe cryptographic provisions

Notwithstanding the output of ETSI GR F5G 010 [i.3] there is a general threat arising from the development of quantum computers. As described in ETSI EG 203 310 [i.7] quantum computers are an existential threat to many common forms of asymmetric cryptography, and a critical threat to common forms of symmetric cryptography, and a substantial threat to many key management and distribution algorithms.

All algorithms used in F5G should be provisioned as quantum safe.

NOTE 1: As of the time of preparation of the present document a small set of algorithms has been selected by NIST for further analysis but there is no consensus on the selection of quantum safe algorithms suited to F5G.

All devices in F5G with a cryptographic function shall ensure that the cryptographic facility is "crypto agile" both within the same class of algorithms, and to allow for migration to an alternative class of algorithm.

NOTE 2: Crypto-agility in a single class of algorithms addresses the use of alternative curves in ECDSA, or alternative key sizes, as well as changing modes of operation in block ciphers (e.g. moving between CTR mode and GCM mode for AES). In the wider application of crypto-agility to move between algorithm classes this includes moving from conventional asymmetric modes (e.g. RSA, ECDSA) to modes based on, for example, codes, hashes, lattices and so forth (e.g. NTRU, FALCON).

NOTE 3: It is acknowledged that some quantum safe cryptographic operations, for asymmetric cryptography, require substantially more processing and longer keys, resulting in larger signature sizes, than more conventional cryptographic measures. This may impact the physical elements of an HSM and appropriate provisions for crypto-agility may not be realisable.

Annex B (informative): The role of trust in security assurance

B.1 Trust as a synonym for security

The role of trust in any form of security assurance is complex and depends on the trusting entity. In a conventional Public Key Infrastructure (PKI) the entire set of assertions is only secured insofar as the recipient has trust that every link in the chain has taken steps to protect their private key.

One view is that trust is a synonym for security:

- Without trust there is no security.
- With proof of security trust can be reinforced.

NOTE: A detailed analysis of trust can be found in ETSI GS NFV-SEC 003 [i.14] and the text in the present document has generalized some of the text from that source for application in the F5G environment.

The preferred model of trust, and the one defined in the present document for F5G, is to begin with the assumption that prior to verification no entity is trusted, i.e. to assume at initialization that the entire network is untrusted. Any physical network element can host a number of possible functions, represented in ETSI TS 103 486 [i.17] as attributes, that can be attested to.

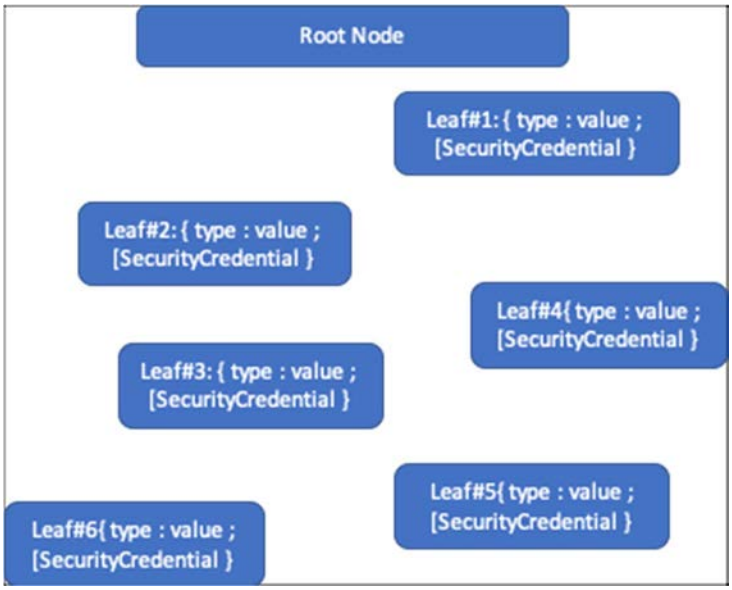

Figure B.1: Unconnected set of attributes (from ETSI TS 103 486 [i.17])

Figure B.1 illustrates a set of attributes for Alice (representing an F5G network element or service) that are attested to by a recognised authority, but which are not organised into an Authority-Attribute tree as defined in ETSI TS 103 486 [i.17]. For application to F5G an attribute is modelled as any application in any of the F5G planes, the root node for F5G is modelled as the attestable identity associated to the HSM of the physical equipment.

B.2 Scope of trust

Within a conventional layered communications architecture the concept of trust is also layered and the convention is that direct trust relationships should not extend beyond the following bounds:

- Trust within an architectural layer (peer to peer).
- Trust of the adjacent architectural layer (Layer N trusts information from layer N-1).

A general model for trust follows the Identity Management (IdM) model that a relying party has to have reasonable confidence that assertions made by the principal (the person declaring their identity) are legitimate and do no harm to the relying party. In order to achieve this in the IdM model the relying party generates an explicit trust relationship with the identity manager prior to any processing related to the principal. The AAT model presented in ETSI TS 103 486 [i.17] and adopted in the present document extends the IdM model by ensuring that any capability on any equipment can be validated by any relying party.

B.3 Models of trust

There are multiple models for trust that determine how Alice establishes trust with Bob. It is recognized that there are few normative standards for trust management and consequently no real tests of trust.

1) Delegated trust

   - The base scenario for delegated trust is that Alice needs to establish a trust relationship with Bob, but lacks some or all of the necessary capabilities to evaluate the appropriate level of trust.
   - Where Alice, the relying party, is unable to evaluate the appropriate level of trust for a relationship with Bob the principal, Alice may choose to delegate the decision to another entity Charles, the identity manager, which is in a better position to make such a decision. In this case, there should be an explicit element to the trust relationship from Alice to Charles that explicitly states that Alice is happy for Charles to make such decisions on behalf of Bob, or components of Bob's type.
   - In this model Charles has been delegated to act as the trust decision maker by Alice on how to treat Bob.

2) Collaborative trust

   - Collaborative trust involves two or more entities (Alice and Charles) working together to decide whether to trust another (Bob). The goal may be for both Alice and Charles to have a trust relationship with Bob, or just one of them. The expectation is that Alice and Charles may have different information available to them which will help them to make a more informed decision about the trust relationship with Bob.
   - The expectation with collaborative trust is that contexts of trust will be shared, but parameters may be different. There should also be opportunities for Alice and Charles to communicate if trust levels - or the parameters on which they are based - change, so that re-evaluation can be performed by all relevant parties.

3) Transitive trust

   - Transitive trust is the decision by Alice to trust Bob because Charles trusts Bob. Transitive trust varies from delegation of trust as Charles may be unaware of Alice's reliance on the Charles-Bob trust relationship and Charles is not party to, or aware of, the resulting trust relationship between Alice and Bob.
   - This model is the dominant one in PKI based trust systems.

4) Reputational trust

   - Reputational trust is a specific instance of transitive trust, where entity A takes a view on the trustworthiness of C based on a rating of B's trust relationship with C. Usually, there will be many other entities that trust C (say D, E, F, G, etc.), and some algorithm will be applied to the various ratings published by these entities in order to allow A to make a decision about trusting B. This algorithm may be applied by A (in which case A needs access the ratings of the various parties C, D, E, F, G, etc.) or by a third party). A distinguishing point about this type of transitive trust is that it is almost always explicit: the entities C, D, E, F, G, etc. are likely to be aware that they are participating in a reputational trust scheme.

NOTE: For assessment of reputational trust the parties B, D, E, F, G, etc. may be representations of the relationship between A and C over time, such that as A and C interact more often over time they generate more trust in each other.

B.4 Evaluation or testing of trust

Testing of trust is difficult conceptually but if the model of trust (for each of the models identified in clause B.3) is translated to the provision of artefacts, such as attestation tickets (e.g. Kerberos or PKCs in an X.509 PKI) then evaluation may be as straightforward as signature verification, and testing that expired or revoked tickets/certificates are handled appropriately.

In a wider model, i.e. not just based on Kerberos or PKC/PKI there are many methods that can be used for trust evaluation, and the choice will depend on available resources and the threats and risks relevant to the entity and the specific deployment. Notwithstanding the lack of core standards the approaches and techniques available for trust tests and evaluation include:

- Reputational approaches: evaluating across a set of different elements, leading to a calculation of "reputation".
- Game theoretical approaches.
- Probabilistic approaches.
- Look-up tables.

Many of the issues that need to be addressed revolve around establishment, re-establishment or revocation of trust. The requirement to re-evaluate trust may be prompted by a variety of different events, including time-based contexts such as a time-out or set frequency. The list below addresses events that may be associated with life cycle events, and acts to allow a categorization and simplification to a smaller set of well-defined trust use cases:

- Disappearance of an entity
- Appearance of an entity
- Movement of an entity - e.g. migration
- Duplication of an entity
- Re-configuration of an entity
- Changes to the description of trust measures
- Changes to the repudiation of roots of trust

B.5 Invalidating trust

There are some cases where trust relationships are invalidated on purpose:

- Notification from the trusted entity that it should no longer be trusted - this is most likely due to an expected destruction, decommissioning or retirement, but could be if the entity believes that it has been compromised.
- Notification from another entity up the chain of trust that a trust relationship should be invalidated.

In these cases, the trusting entity should generally not attempt to re-establish the trust relationship.

B.6 Development of a trust manager

There are many occasions when placing significant trust determination logic in entities - which are generally of very specific function, and may be designed to be as lightweight as possible - is not appropriate.

Benefits of a Trust Manager:

- Less logic required by other entities within the deployment.
- Can act as a *deus ex machina*, providing information across different architectural layers.

- Act as an interface between different administrative domains and operators.
- Provide historical data about entities that are more long-lived than the trusting entity.

Drawbacks of a Trust Manager:

- Single point of failure.
- Single point of attack.
- May require communications channels across architectural boundaries which are not easily maintained.
- Encourages "crunching" of trust contexts in a smaller set of implicit contexts.
- Encourages assumptions that all entities share the same trust contexts.

Annex C (informative): Bibliography

C.1 ETSI documents in development at time of publication

The following documents are not explicitly cited in the present document as normative or informative but may, on publication, offer specific mechanisms to be implemented in F5G.

- DTS/CYBER-0086 (TS): "Security provisions for the management of Optical Network devices and services".
- DTS/CYBER-0093 (TS): "Security provisions in optical transport network devices".
- DTS/CYBER-0092 (TS): "Security provisions in optical access network devices".
- ETSI GS ETI 003: "Encrypted Traffic Integration (ETI); Integration strategies and techniques".
- ETSI GR ETI 002: "Encrypted Traffic Integration (ETI); Requirements definition and analysis".

C.2 Data encoding and error correction schemes

The use of Cyclic Redundancy Codes (CRCs) as part of a forward error correction scheme is widely discussed in literature and the following documents offer the reader useful background on the topic. The expectation is that channel encoding to maximize reliability is deployed but such provisions are not specifically addressed in the present document.

- ECMA-182: "Data interchange on 12,7 mm 48-track magnetic tape cartridges - DLT1 format".
- ETSI TS 100 909: "Digital cellular telecommunications system (Phase 2+); Channel coding".
- ETSI TS 125 427: "Universal Mobile Telecommunications System (UMTS); UTRAN Iub/Iur interface user plane protocol for DCH data streams".
- MacWilliams, F. J., Sloane, N. J. A. (1977): "The Theory of Error-Correcting Codes", New York, NY: North-Holland Publishing Company.
- ETSI EN 300 392-2: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)".
- Reed, Solomon: "Polynomial codes over certain finite fields".

C.3 Other security documents

- NIST Special Publication 800-207: "Zero Trust Architecture".

History

Document history		
V1.1.1	January 2023	Publication