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

GROUP SPECIFICATION

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

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 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	Nth 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.

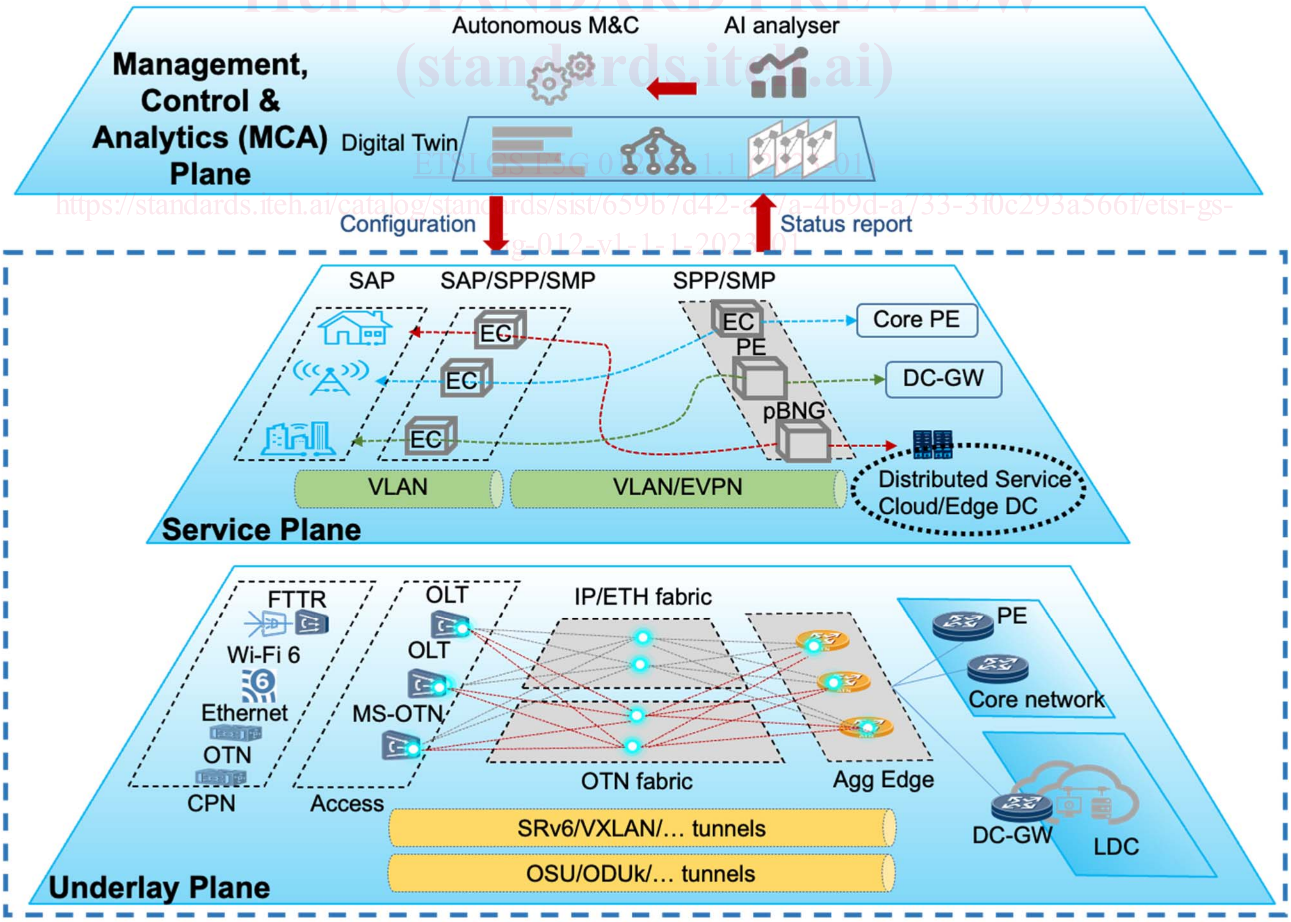

Figure 4.1: F5G network architecture from ETSI GS F5G 004 [i.2]

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.