

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1811

(04/2021)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

IMT-2020 Security

Security guidelines for applying quantum-safe algorithms in IMT-2020 systems

Recommendation ITU-T X.1811

ITU-T

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
IMT-2020 SECURITY	X.1800–X.1819

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1811

Security guidelines for applying quantum-safe algorithms in IMT-2020 systems

Summary

Recommendation ITU-T X.1811 identifies threats raised by quantum computing to International Mobile Telecommunications-2020 (IMT-2020) systems through assessing the security strength of currently used cryptographic algorithms. This Recommendation briefly reviews quantum safe algorithms, including both symmetric and asymmetric types, and provides guidelines for applying quantum safe algorithms in IMT-2020 systems.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1811	2021-04-30	17	11.1002/1000/14454

Keywords

5G system, asymmetric algorithm, IMT-2020 system, quantum computer, quantum-safe algorithm, symmetric algorithm.

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2021

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Recommendation.....	2
4 Abbreviations and acronyms	2
5 Conventions	5
6 Overview	5
7 Introduction to security components of IMT-2020 systems.....	6
7.1 Security of the infrastructure layer	7
7.2 Security of the network layer	8
7.3 Security of the management plane	15
7.4 Summary of the cryptographic algorithms used in IMT-2020 system.....	15
8 Security assessment of IMT-2020 systems under quantum computing	16
8.1 Threats to conventional cryptographic algorithms	16
8.2 Prediction of the timeline for large-scale quantum computer	18
8.3 Impacts on IMT-2020 systems	18
9 Quantum-safe cryptographic algorithms	21
9.1 Quantum-safe symmetric key algorithms.....	21
9.2 Quantum-safe asymmetric key algorithms.....	21
10 Guidelines for usage of quantum-safe cryptographic algorithms in IMT-2020 systems.....	22
10.1 Message size	22
10.2 IPsec, TLS and DTLS.....	23
10.3 Infrastructure layer	23
10.4 IMT-2020 access network	23
10.5 IMT-2020 core network	24
Appendix I – Overview of IMT-2020 system.....	25
I.1 General architecture.....	25
I.2 SDN	26
I.3 Access network.....	26
I.4 Core network	27
I.5 Management plane.....	29
Appendix II – Quantum-safe asymmetric key cryptographic algorithms.....	30
II.1 Lattice-based algorithms	30
II.2 Hash-based algorithms	30

	Page
II.3 Code-based algorithms	30
II.4 Multivariate algorithms	30
II.5 NIST standardization of post quantum cryptography	30
Appendix III – Impact of quantum computing on common cryptographic algorithms	33
Appendix IV – Assessment criteria for quantum-safe cryptography.....	34
IV.1 Security.....	34
IV.2 Cost.....	35
IV.3 Algorithm and implementation characteristics.....	36
Bibliography.....	37

Introduction

The International Mobile Telecommunications-2020 (IMT-2020) system promises to support a wide range of services with diverse performance requirements in order to form a fully connected society. To achieve this challenging goal, a number of innovative technologies have been developed in the IMT-2020 system, such as network slicing, the software-defined network, virtualized network function and central unit/distributed unit (CU/DU) separation. Security measures are fundamental to ensuring the normal operation of the IMT-2020 system. Besides the use of symmetric cryptographic algorithms, those that are asymmetric, have been deployed in the IMT-2020 system.

A large-scale quantum computer raises security concerns to current widely used symmetric and asymmetric cryptographic algorithms. The latter no longer provide security in the quantum-computing era. Furthermore, symmetric cryptographic algorithms have to double their key lengths to resist quantum-computing attacks. For this, deployment of quantum-safe cryptographic algorithms is highly desirable in the IMT-2020 system.

In this Recommendation, the IMT-2020 system and its security architecture are briefly surveyed. The threats to IMT-2020 systems due to quantum computers are assessed. Quantum-safe algorithms are briefly reviewed, but their details are not specified in this Recommendation. Security guidelines will be included in a high-level Recommendation to adapt quantum-safe algorithms to IMT-2020 systems. This Recommendation is intended to provide the guidelines for the application of quantum-safe symmetric and asymmetric algorithms to the IMT-2020 system, as well as the alignment of security levels between quantum-safe symmetric and asymmetric algorithms.

Recommendation ITU-T X.1811

Security guidelines for applying quantum-safe algorithms in IMT-2020 systems

1 Scope

This Recommendation covers:

- an introduction to the security architecture of International Mobile Telecommunications-2020 (IMT-2020) systems;
- a security assessment of IMT-2020 systems when commercial quantum computers are available;
- a specification of the usage of quantum-safe algorithms in IMT-2020 systems.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- [ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
- [ITU-T X.1038] Recommendation ITU-T X.1038 (2016), *Security requirements and reference architecture for software-defined networking*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication [b-ITU-T Y.2014]: A property by which the correct identity of an entity or party is established with a required assurance. The party being authenticated could be a user, subscriber, home environment or serving network.

3.1.2 authentication protocol [b-ITU-T X.1254]: A defined sequence of messages between an entity and a verifier that enables the verifier to perform authentication of an entity.

3.1.3 authorization [b-ISO 7498-2]: The granting of rights, which includes the granting of access based on access rights..

3.1.4 availability [ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

3.1.5 credential [b-ITU-T X.1252]: A set of data presented as evidence of a claimed identity and/or entitlements.

3.1.6 confidentiality [ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.1.7 data integrity [ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.8 privacy [ITU-T X.800]: The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

3.1.9 key hierarchy [b-ITU X.1196]: A tree structure that represents the relationship of different keys. In a key hierarchy, a node represents a key used to derive the keys represented by the descendent nodes. A key can only have one precedent, but may have multiple descendent nodes.

3.1.10 network function virtualization; NFV [b-ISO/IEC TR 22417]: Technology that enables the creation of logically isolated network partitions over shared physical networks so that heterogeneous collections of multiple virtual networks can simultaneously coexist over the shared networks.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

4G	fourth Generation
AES	Advanced Encryption Standard
AES-CBC	Advanced Encryption Standard-Cipher Blocker Chaining
AES-GCM	Advanced Encryption Standard-Galois Counter Mode
AES-GMAC	Advanced Encryption Standard-Galois Message Authentication Code
AF	Application Function
AKA	Authentication and Key Agreement
AMF	Access and Mobility management Function
API	Application Programming Interface
ARPF	Authentication credential Repository and Processing Function
AS	Access Stratum
AUSF	Authentication Server Function
AV	Authentication Vector
CEK	Content Encryption Key
CM	Configuration Management
CP	Control Plane
CU/DU	Central Unit/Distributed Unit
DH	Diffie-Hellman
DHE	Diffie-Hellman Ephemeral
DNSSec	Domain Name System Security extensions
DSA	Digital Signature Algorithm
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
ECC	Elliptic-Curve Cryptography

ECDH	Elliptic Curve Diffie-Hellman
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDLP	Elliptic Curve Discrete-Log Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
ECP	Extended Cutting Plane
eMBB	enhanced Mobile Broadband
ESP	Encapsulating Security Payload
FM	Fault Management
GKDF	Generic Key Derivation Function
gNB	NR Node B
GUTI	Globally Unique Temporary Identifier
HMAC	Hash-based Message Authentication Code
HKDF	HMAC-based Extract-and-Expand Key Derivation Function
ICV	Integrity Check Value
IPsec	Internet Protocol Security
IKE	Internet Key Exchange
IKEv2	Internet Key Exchange version 2
IMT-2020	International Mobile Telecommunications-2020
IP	Internet Protocol
IPX	IP exchange
JOSE	Javascript Object Signing And Encryption
JSON	JavaScript Object Notation
JWE	JSON Web Encryption
JWS	JSON Web Signature
KDF	Key Derivation Function
KEM	Key Encapsulation Mechanism
LTE	Long-Term Evolution
LWE	Learning With Errors
MAC	Message Authentication Code
mIoT	massive Internet of Things
mMTC	massive Machine-Type Communication
MNO	Mobile Network Operator
MODP	Modular exponential
MPLS	Multiprotocol Label Switching
N3IWF	Non-3GPP Interworking Function
NAS	Non-Access Stratum

NDS	Network Domain Security
NEF	Network Exposure Function
NF	Network Function
NFV	Network Function Virtualization
NFVI	Network Function Virtualization Infrastructure
NG-RAN	Next Generation-Radio Access Network
NP	Non-deterministic Polynomial time
NRF	NF Repository Function
NSSF	Network Slice Selection Function
NTRU	Nth degree Truncated Polynomial Ring
PCF	Policy Control Function
PDCP	Packet Data Convergence Protocol
PKI	Public-Key Infrastructure
PKE	Public-Key Encryption
PM	Performance Management
PRF	Pseudo-Random Function
PSK	Pre-Shared Key
RLC	Radio Link Control
R-LWE	Ring Learning With Errors
RRC	Radio Resource Control
RSA	Rivest, Shamir and Adelman
PLMN	Public Land Mobile Network
PQC	Post-Quantum Cryptography
SBA	Service-Based Architecture
SDAP	Service Data Adaptation Protocol
SDN	Software-Defined Network
SEAF	Security Anchor Function
SEPP	Security Edge Protection Proxy
SHA	Secure Hash Algorithm
SIDF	Subscription Identifier De-concealing Function
SIDH	Supersingular-Isogeny Diffie–Hellman
SIKE	Supersingular Isogeny Key Encapsulation
SMF	Session Management Function
SSH	Secure Shell
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
SVP	Shortest Vector Problem

TLS	Transport Layer Security
TM	Trace Management
UDM	Unified Data Management
UDR	User Data Repository
UE	User Equipment
UOV	Unbalanced Oil and Vinegar
UP	User Plane
UPF	User Plane Function
URLLC	Ultra-Reliable and Low-Latency Communication
USIM	Universal Subscriber Identity Module
VNF	Virtual Network Function
WLAN	Wireless Local Area Network
XMSS	extended Merkle Signature Scheme

5 Conventions

In this Recommendation:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "**is prohibited from**" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Overview

The IMT-2020 mobile communication technology is positioned to meet the business needs of the year 2020 and beyond. Security architecture is key to enabling normal operation of an IMT-2020 network. In fourth generation/long-term evolution (4G/LTE), only symmetric algorithms are utilized to protect signalling and user data. In addition to these, IMT-2020 systems introduce asymmetric algorithms to protect not only subscriber identifiers, but also communication between mobile network operators (MNOs).

Recently (as of September 2020), IBM has announced the 50 qubit quantum computer [b-QC1]. This breakthrough has dispelled the original anticipation that large-scale quantum computers would be on the market in 20 years. The new report [b-QC2] now estimates that 10 years is a realistic forecast for their availability.

The security of public-key cryptographic algorithms depends on the difficulty of computational problems, such as integer factorization or the discrete logarithm problem over various groups. It is showed that quantum computers can efficiently solve each of these problems [b-Shor 1997], thereby making all public-key cryptosystems based on such assumptions impotent. Thus, a sufficiently

powerful quantum computer will put at risk many forms of modern cryptosystems, such as key exchange, encryption and digital authentication.

Quantum computers will affect the security strength of symmetric and asymmetric algorithms to a different degree. Symmetric cryptographic strength will be halved, e.g., an advanced encryption standard (AES) with 128 bit keys giving 128 bit strength will be reduced to that of 64 bits, whereas many commonly used asymmetric algorithms, such as Rivest, Shamir and Adelman (RSA), digital signature algorithm (DSA) and elliptic-curve cryptography (ECC), will offer no security.

The IMT-2020 system aims to provide a wide range of services with different performance requirements. The services provided in IMT-2020 networks can be classified into enhanced mobile broadband (eMBB), massive Internet of things (mIoT) and ultra-reliable and low-latency communications (URLLCs).

The IMT-2020 system introduces a number of innovative technologies, such as network slicing, network function virtualization (NFV), the software-defined network (SDN) and service-based architecture (SBA). These technologies make the IMT-2020 system a flexible platform enabling new business cases and integrating vertical industries. On the other side, they make the security architecture of the IMT-2020 system much more complicated than previous mobile network generations.

There is a high desire to study how to protect communications in IMT-2020 systems by using quantum-safe algorithms. This is because it is likely that commercial quantum computers will become available within the lifecycle of IMT-2020 systems. Currently, the key length of symmetric algorithms specified for IMT-2020 systems is 128 bits. The 3rd Generation Partnership Project (3GPP) has just initiated a study item to research how to apply 256 bit key length symmetric algorithms to IMT-2020 systems [b-3GPP TR 33.841]. However, to date there has been no organization to study how to apply quantum-safe asymmetric algorithms to IMT-2020 systems. Some adaptation has to be made when quantum-safe cryptographic algorithms are used in IMT-2020 systems, since they have a longer key length than those used in classical cryptography. Moreover, there is a need to study how keys of different size coexist in IMT-2020 systems, since it is impossible to replace all classical algorithms with those that are quantum-safe overnight. A transition to quantum-safe cryptography in IMT-2020 systems should be considered early, so that any information that is later compromised by quantum cryptanalysis is no longer sensitive.

In this Recommendation, the threats to IMT-2020 systems due to quantum computers are assessed. Quantum-safe algorithms are briefly reviewed, but their details are not specified in this Recommendation. The security guidelines recommend, at a high level, the adaptation of quantum-safe algorithms to IMT-2020 systems. This Recommendation provides the comprehensive guidelines to the application of quantum-safe symmetric and asymmetric algorithms to IMT-2020 systems, as well as the alignment of security levels between quantum-safe symmetric and asymmetric algorithms.

7 Introduction to security components of IMT-2020 systems

This clause provides background information for the security components of IMT-2020 systems, which have been specified in ITU-T, 3GPP, ETSI, IETF, etc.

A communication system should be able to provide some of the following security services to ensure the security of the system or data transmission [ITU-T X.800]: access control (authorization); authentication; privacy; confidentiality; data integrity; non-repudiation; and availability.

Security services could be achieved by using cryptographic or non-cryptographic mechanisms. This Recommendation focuses on the former, since it studies the application of quantum cryptographic algorithms to IMT-2020 systems.

In accordance with the architecture of IMT-2020 systems introduced in Appendix I, the security architecture of IMT-2020 systems can be described in three layers: infrastructure layer, network layer, and management plane.

7.1 Security of the infrastructure layer

The infrastructure layer is the common base to support the upper layer in IMT-2020 systems, which encompasses SDN and network function virtualization infrastructure (NFVI) layer.

7.1.1 Security of SDN

SDN technology is used for data delivery in IMT-2020 due to its dynamic and flexible management of traffic flows. The security architecture of SDN is specified in [ITU-T X.1038], which is simply illustrated in Figure 1.

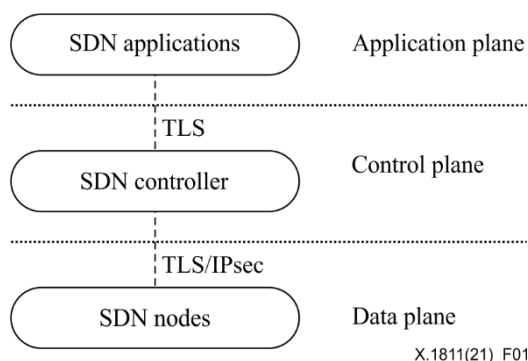


Figure 1 – Security architecture of SDN

[ITU-T X.1038] specifies the following recommendations relating to cryptographic algorithms and protocols.

The deployment of the transport layer security (TLS) [b-IETF RFC 5246] protocol is recommended to be put in place in the interface between the SDN application and the SDN controller. Based on TLS, the SDN application and the SDN controller authenticate each other and agree upon the session key; in addition, data confidentiality and data integrity over the application control interface are ensured.

The deployment of the TLS [b-IETF RFC 5246] protocol or Internet protocol security (IPSec) protocols ([b-IETF RFC 4301], [b-IETF RFC 4303], [b-IETF RFC 4835]) is recommended to be put in place in the interface between the SDN controller and the SDN node. Based on TLS or IPsec, the SDN node and the SDN controller authenticate each other and agree upon the session key; in addition, data confidentiality and data integrity over the control note interface are ensured.

Authentication mechanisms could be based on either a pre-shared key (PSK) [b-IETF RFC 4279] [b-IETF RFC 4306] or a certificate [b-IETF RFC 4306] and [b-IETF RFC 5246]. Either RSA [b-ONF TR-511] or digital signature algorithms can be applied in certificate-based authentication. The Diffie-Hellman (DH) or elliptic curve Diffie-Hellman (ECDH) key exchange protocol can be implemented in the context of TLS or IPsec to agree upon the shared key between the two entities.

Cryptographic algorithms used for data encryption could be AES [b-NIST FIPS 197], Blowfish [b-Schneier] or 3DES [b-NIST SP 800-67]. Cryptographic algorithms used for data integrity mechanisms could be message authentication code (MAC) [b-IETF RFC 2104], hash-based message authentication code (HMAC) [b-IETF RFC 2104] or digital signature [b-NIST FIPS 186-4].

7.1.2 Security of the NFVI layer

The NFVI layer supports the running of virtual network functions (VNFs), whose structure is depicted in Figure 2.

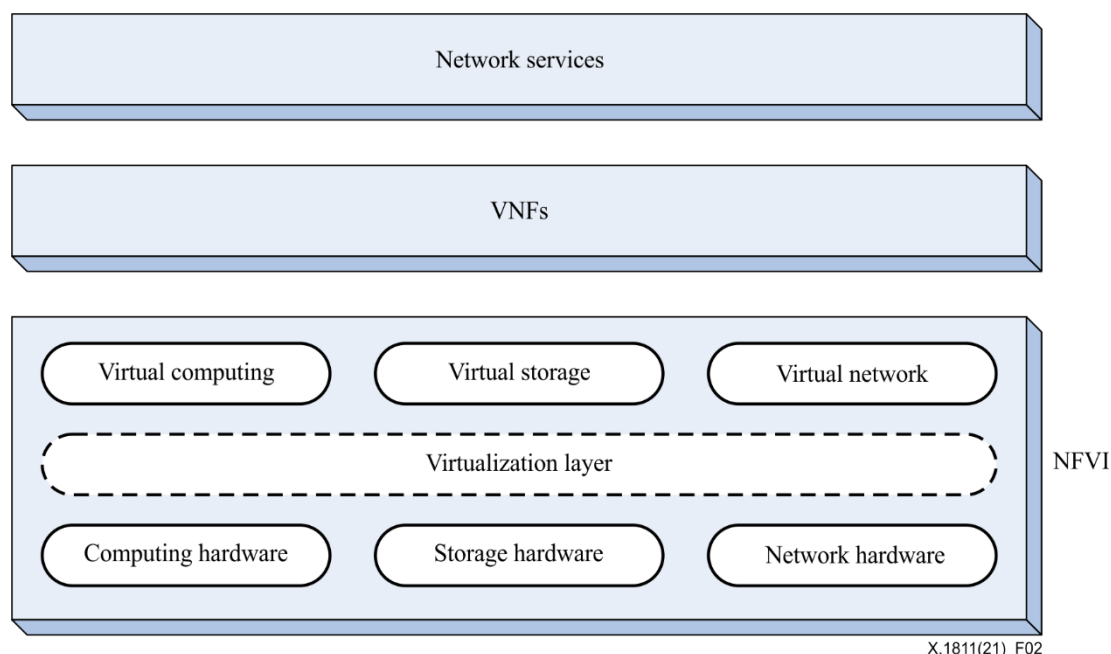


Figure 2 – NFVI structure (adapted from Figure 1 of [b-ETSI GS NFV 002])

According to [b-ETSI GS NFV-SEC 012], the NFVI shall support the following security functions to ensure the security of VNFs running on top of it: secure logging; operating system-level access and confinement control; physical controls and alarms; authentication controls; access controls; communications security; attestation; hardware-mediated execution enclaves; hardware-based root of trust; self-encrypting storage; direct access to memory; hardware security modules; and software integrity protection and verification. For this, the NFVI shall implement the following cryptographic algorithms [b-ETSI GS NFV-SEC 012]:

- 1) hashing algorithms: SHA-256, SHA-384, AES128-GMAC, HMAC-SHA128, HMAC-SHA256, HMAC-SHA384;
- 2) encryption algorithms: AES-CBC-128, AES-GCM-128 (16 octet integrity check value (ICV)), AES-CBC-256, AES-GCM-256 (16 octet ICV);
- 3) signature: RSA 2048, RSA 3072, RSA 4096, ECDSA-256 (secp256r1), ECDSA-384 (secp384r1);
- 4) public-key infrastructure (PKI): RSA 2048, RSA 3072, RSA 4096, id-ecPublicKey (secp256r1);
- 5) key exchange: DH group 14 (2 048 bit modular exponential (MODP)), DH group 19 (256 bit random extended cutting plane (ECP) group), DH group 20 (384 bit random ECP group), elliptic curve Diffie-Hellman ephemeral (ECDHE) secp256r1 (P-256), Diffie-Hellman ephemeral (DHE) groups of at least 2048 bits;
- 6) Pseudo-random function (PRF): PRF-HMAC-SHA2-256, PRF-HMAC-SHA2-384.

7.2 Security of the network layer

7.2.1 Security of the access network

The security of the access network [b-3GPP TS 33.501] is intended to ensure that authenticated user equipment (UE) is able to gain access to an IMT-2020 network, the communication between UE and the IMT-2020 network could be protected in a selectable fashion according to MNO security policy.