

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1814

(09/2022)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

IMT-2020 Security

Security guidelines for IMT-2020 communication systems

Recommendation ITU-T X.1814

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 (1)	X.1140–X.1149
Application Security (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.1350–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1399
Distributed ledger technology (DLT) security	X.1400–X.1429
Application Security (2)	X.1450–X.1459
Web security (2)	X.1470–X.1489
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
Cyber Defence	X.1590–X.1599
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
Data protection	X.1770–X.1789
IMT-2020 SECURITY	X.1800–X.1814



Recommendation ITU-T X.1814

Security guidelines for IMT-2020 communication systems

Summary

Connected Internet of things (IoT) devices and mobile applications require wireless network access that is resilient, secure and able to protect individuals' privacy. IMT-2020 communication systems should be designed to meet these high-level requirements. There is a need to define a security framework for IMT-2020 communication systems which could act as a foundation for developing further detailed technical Recommendations on IMT-2020 security topics.

Recommendation ITU-T X.1814 identifies all components related to the security of IMT-2020 communication systems and defines security guidelines for the IMT-2020 communication system. It describes a generic IMT-2020 architecture and its domains. It also identifies threats to and specifies requirements for security capabilities for each component, taking into account unique network features. This Recommendation is based on the 3GPP 5G security architecture.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1814	2022-09-02	17	11.1002/1000/14992

Keywords

Capability, IMT-2020 communication system, multiaccess edge computing, network slicing, network virtualization, security guidelines, threats.

* 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 not 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 2022

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	3
5	Conventions	4
6	Overview of security for the IMT-2020 communication system	4
	6.1 Simplified IMT-2020 architecture.....	4
	6.2 General architecture of IMT-2020 system	5
	6.3 Domains of IMT-2020 system.....	6
	6.4 General security requirements and capabilities	8
7	Components and trustworthiness of the IMT-2020 communication system	10
	7.1 IMT-2020 components	10
	7.2 Trustworthiness of the IMT-2020 communication system	11
8	Threats to components and functions	12
	8.1 Generic threats.....	12
	8.2 Threats to user equipment	14
	8.3 Threats to access networks	15
	8.4 Threats to software-defined networking.....	16
	8.5 Threats to core network	16
	8.6 Threats to network slicing	17
	8.7 Threats to multiaccess edge computing.....	18
	8.8 Threats to network function virtualization	18
	8.9 Threats to management.....	19
9	Requirements for security capabilities related to components and functions.....	19
	9.1 Security capabilities related to user equipment	19
	9.2 Security capabilities related to access network	20
	9.3 Security capabilities related to software-defined networking	21
	9.4 Security capabilities related to core network.....	22
	9.5 Security capabilities related to network slicing.....	22
	9.6 Security capabilities related to multiaccess edge computing	24
	9.7 Security capabilities related to network function virtualization.....	24
	9.8 Security capabilities related to management function.....	24
	Annex A – Security architecture for IMT-2020 communication system.....	26
	Appendix I – Generic network security architecture for providing end-to-end network security.....	27

	Page
Appendix II – Threat of service disruption from a manipulated radio resource control (RRC) connection request and its capability	28
II.1 Overview	28
II.2 Attack scenario	28
II.3 Consequence	29
II.4 Countermeasures	29
Bibliography.....	31

Recommendation ITU-T X.1814

Security guidelines for IMT-2020 communication systems

1 Scope

This Recommendation provides security guidelines for the development of IMT-2020 communication systems. It identifies all components related to the security of an IMT-2020 communication system, i.e., user equipment, access network and core network. It describes a generic IMT-2020 architecture and its domains. It also identifies threats to and specifies requirements on security capabilities for each component, taking into account unique network features such as multiaccess edge computing, software-defined networking, dynamic network function virtualization and network slicing. This Recommendation is based on the 3GPP 5G security architecture.

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

3.1.1 This Recommendation uses the following terms from [ITU-T X.800]:

- access control;
- authentication;
- availability;
- confidentiality;
- data integrity;
- privacy;
- repudiation;
- security service.

In addition, this Recommendation uses the following additional terms defined elsewhere:

3.1.2 control [b-ITU-T X.1408]: Measure that is modifying risk.

NOTE 1 – Controls include any process, policy, device, practice, or other actions which modify risk.

NOTE 2 – Controls may not always exert the intended or assumed modifying effect.

3.1.3 distributed denial-of-service (DDoS) attack [b-ITU-T Y.4807]: Unauthorized access to a system resource or the delaying of system operations and functions in the way of compromising multiple systems to flood the bandwidth or resources of the targeted system, with resultant loss of availability to authorized users.

3.1.4 guideline [b-ITU-T X.1401]: Description that clarifies what should be done and how, to achieve the objectives set out in policies.

3.1.5 network function [b-ITU-T Y.3100]: In the context of IMT-2020, a processing function in a network.

NOTE 1 – Network functions include but are not limited to network node functionalities, e.g., session management, mobility management and transport functions, whose functional behaviour and interfaces are defined.

NOTE 2 – Network functions can be implemented on a dedicated hardware or as virtualized software functions.

NOTE 3 – Network functions are not regarded as resources, but rather any network functions can be instantiated using the resources.

3.1.6 network function virtualization [b-ITU-T X.1811]: 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.

3.1.7 network slice [b-ITU-T Y.3100]: A logical network that provides specific network capabilities and network characteristics.

NOTE 1 – Network slices enable the creation of customized networks to provide flexible solutions for different market scenarios which have diverse requirements, with respect to functionalities, performance and resource allocation.

NOTE 2 – A network slice may have the ability to expose its capabilities.

NOTE 3 – The behaviour of a network slice is realized via network slice instance(s).

3.1.8 orchestration [b-ITU-T Y.3100]: In the context of IMT-2020, the processes aiming at the automated arrangement, coordination, instantiation and use of network functions and resources for both physical and virtual infrastructures by optimization criteria.

3.1.9 security capability [b-ISO 81001-1]: Broad category of technical, administrative, or organizational controls to manage risks to confidentiality, integrity, availability and accountability of data and systems.

3.1.10 supplier [b-ISO 10393]: Organization or person that provides a product or service.

3.1.11 system [b-ISO/IEC 27000]: Applications, services, information technology assets, or other information handling components.

3.1.12 threat [b-ITU-T X.1406]: Potential cause of an unwanted incident, which can result in harm to a system or organization.

3.1.13 virtualized network function [b-ITU-T Y.3150]: A network function whose functional software is decoupled from hardware, and runs on virtual machine(s).

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 domain: A grouping of network entities according to physical or logical aspects that are relevant for an IMT-2020 network.

3.2.2 IMT-2020 communication system: A system of managing IMT-2020 communication processes for IMT-2020 services.

NOTE 1 – 5G is referred to as IMT-2020 in ITU-T context.

NOTE 2 – The IMT-2020 communication system is identical to IMT-2020 system in this Recommendation.

3.2.3 IMT-2020 ecosystem: A set of stakeholders which interact to form a stable functioning IMT-2020 system.

NOTE – This mainly relies on IMT-2020 communication technology, in which a community of living organisms contains producers, consumers and suppliers who contribute vast amounts of products, technology and expertise to make an IMT-2020 system work on different levels such as infrastructure, network, platform, service and application.

3.2.4 IMT-2020 service: A benefit provided by the IMT-2020 ecosystem.

3.2.5 flow table overflow attack: An attack that consumes flow tables that forward and process packets of flows, which results in no space left for other flows to install flow rules and thus incurs network denial-of-service (DoS).

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

4G	Fourth Generation of Mobile Communication Technology
AMF	Access and Mobility management Function
API	Application Programming Interface
AUSF	Authentication Server Function
C-PDU	Control Protocol Data Unit
CU/DU	Central Unit/Distributed Unit
DCI	Data Centres Interconnect
DDoS	Distributed Denial-of-Service
DoS	Denial-of-Service
eMBB	enhanced Mobile Broadband
FAT	File Allocation Table
IMSI	International Mobile Subscriber Identity
IMT-2020	International Mobile Telecommunications-2020
IoT	Internet of Things
LTE	Long-Term Evolution
MAC	Message Authentication Code
MEC	Multiaccess Edge Computing
MEHW	Mobile Equipment Hardware
mIoT	massive Internet of Things
mMTC	massive Machine-Type Communications
MNO	Mobile Network Operator
NAS	Non-Access Stratum

NF	Network Function
NFV	Network Function Virtualization
NFVI	Network Functions Virtualization Infrastructure
NRF	Network Function Repository Function
OAM	Operation, Administration and Management
O&M	Operations and Management
PII	Personally Identifiable Information
PSK	Pre-Shared Key
RA/CA	Registration Authority and Certification Authority
RRC	Radio Resource Control
SBA	Service-Based Architecture
SBI	Service-Based Interface
SDN	Software-Defined Networking
SMF	Session Management Function
SQL	Structured Query Language
SSL	Secure Sockets Layer
TA	Trust Anchor
TLS	Transport Layer Security
TMSI	Temporary Mobile Subscriber's Identity
TPM	Trusted Platform Module
UDM	Unified Data Management
UE	User Equipment
UICC	Universal Integrated Circuit Card
URLLC	Ultra-Reliable and Low-Latency Communications
USIM	Universal Subscriber Identity Module
VM	Virtual Machine
VNF	Virtual Network Function
VoIP	Voice over Internet Protocol

5 Conventions

In this Recommendation, the keyword "should" indicates a specification which is recommended but which is not absolutely required. Thus, this specification need not be present to claim conformance.

6 Overview of security for the IMT-2020 communication system

6.1 Simplified IMT-2020 architecture

This clause gives an overview of security for the IMT-2020 communication system. Connected mobile devices and mobile applications require wireless network access that is resilient, secure and

trustworthy. The IMT-2020 communication system should be designed to meet these high-level requirements.

An IMT-2020 communication system consists of devices connected to an IMT-2020 access network, which in turn is connected to the rest of the system, which is called an IMT-2020 core network.

Figure 1 shows a simplified 3GPP 5G system architecture. The IMT-2020 access network includes 3GPP radio base stations and/or a non-3GPP access network. The IMT-2020 core network architecture is significantly better than 4G in terms of being able to support cloud implementation and the Internet of things (IoT), with major improvements in network slicing and service-based architecture (SBA).

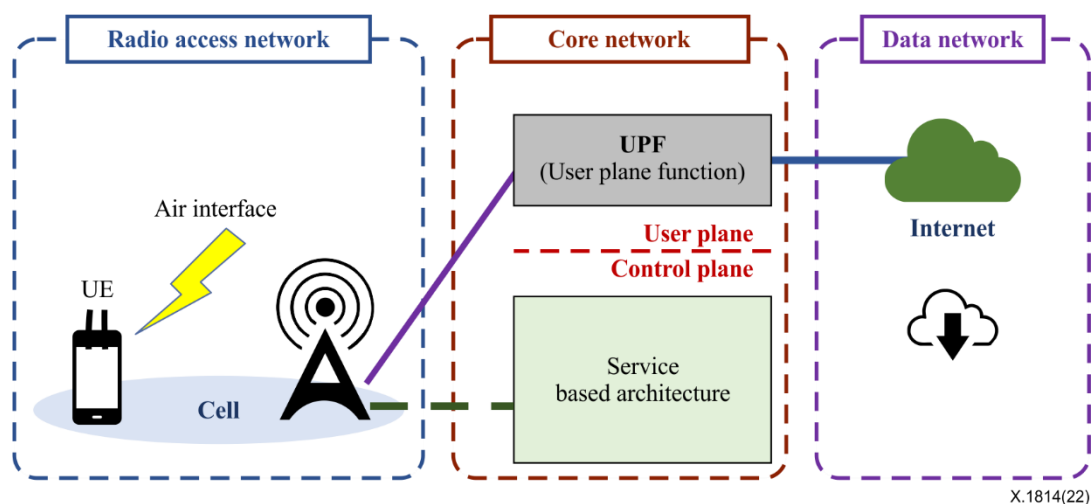


Figure 1 – Simplified IMT-2020 architecture

6.2 General architecture of IMT-2020 system

The IMT-2020 system aims at providing a wide range of services with different performance requirements. The services provided in IMT-2020 networks can be classified into three categories according to 3GPP specifications: (1) Enhanced mobile broadband (eMBB) supports higher data rates and higher user mobility than the fourth generation of mobile communication technology/long term evolution network (4G/LTE); (2) Massive Internet of Things (mIoT) provides massive machine type communications; (3) Ultra-reliable and low-latency communications (URLLC) support the mission critical services which require higher reliability and lower latency. The IMT-2020 system is to be a flexible platform enabling new business cases and integrating verticals such as automotive, manufacturing, energy, eHealth and entertainment. Moreover, the deployment and maintenance of the IMT-2020 system is to be easier compared with the previous generations of mobile networks. To address these challenging requirements, the IMT-2020 system has introduced a number of innovation technologies, such as network slicing, network function virtualization (NFV), software-defined networking (SDN), SBA and central unit/distributed unit (CU/DU) separation.

A general architecture of the IMT-2020 system [b-ITU-T X.1811] is illustrated in Figure 2, which includes the transport layer, network layer, service layer and management plane according to the required functionalities.

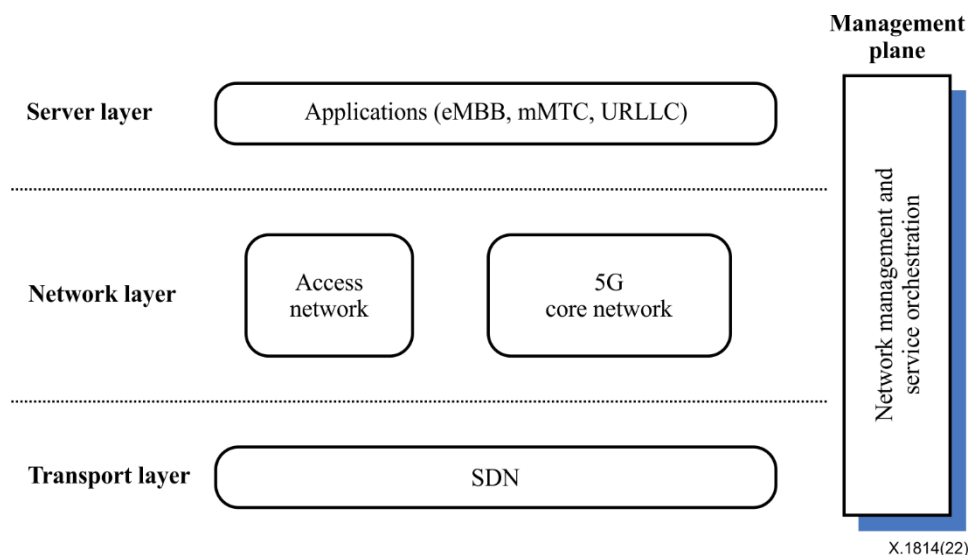


Figure 2 – General architecture of IMT-2020 system [b-ITU-T X.1811], [b-TS 33.501]

- **Transport layer:** This is used to transport packets between the source and the destination. Besides legacy transport technologies (e.g., Multiprotocol label switching), the IMT-2020 system has introduced SDN technology for higher transport speeds and easier adoption of service requirements.
- **Network layer:** This is composed of the access network and the core network. The former allows UE access to the IMT-2020 network. The latter is designed with a SBA to allow for extensibility and simplicity. It is made up of a number of network functions to support data connectivity and service deployment. Examples of network functions include the authentication server function (AUSF), access and mobility management function (AMF), and session management function (SMF).
- **Service layer:** This consists of the applications running on the top of the IMT-2020 system, which may be eMBB, mMTC or URLLC applications.
- **Management plane:** This is responsible for the network management and service orchestration.

6.3 Domains of IMT-2020 system

IMT-2020 security should be defined according to domains, layers, security requirements and security capabilities.

A domain is a grouping of network entities according to physical or logical aspects that are relevant for an IMT-2020 network. The concept of a slice domain is used to capture network slicing aspects. It can represent different functionalities, services and actors in IMT-2020 networks. Figure 3 represents the typical IMT-2020 domain.