

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.1813

(09/2022)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

IMT-2020 Security

Security and monitoring requirements for operation of vertical services supporting ultra-reliability and low-latency communication (URLLC) in IMT-2020 private networks

Recommendation ITU-T X.1813

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.1819



Recommendation ITU-T X.1813

Security and monitoring requirements for operation of vertical services supporting ultra-reliability and low-latency communication (URLLC) in IMT-2020 private networks

Summary

Recommendation ITU-T X.1813 specifies the security requirements for the operation of vertical services supporting ultra-reliable low-latency communications URLLC in an IMT-2020 private network. It identifies threats and risks which arise when providing vertical services supporting URLLC in an IMT-2020 private network and describes security deployment scenarios of the IMT-2020 private network for operation of vertical services supporting URLLC. Monitoring of communication contents is out of the scope of this Recommendation.

IMT-2020 private network, also regarded as IMT-2020 non-public network (NPN), is intended for the sole use of a private entity such as an enterprise and may be deployed in a variety of configurations, utilizing both virtual and physical elements. It will deliver on speed, low latency and other benefits promised by the IMT-2020 to support next-generation applications.

In vertical services for smart factories and smart cities that use a private IMT-2020 network, many Internet of things (IoT) devices use massive machine-type communications (mMTC) and ultra-reliable low-latency communications (URLLC). These communications can be exposed to security threats and their associated risks. In addition, these threats can deteriorate the stable operation of the vertical services supporting URLLC. It cannot be guaranteed when the performance of vertical services is degraded due to these risks.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1813	2022-09-02	17	11.1002/1000/14991

Keywords

DPI, endpoint detection and response, MEC, NPN, network monitoring, performance, private IMT-2020 network, security, UPF.

* 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	2
5	Conventions	3
6	Overview	3
7	Threats to vertical services supporting URLLC in IMT-2020 private networks.....	5
8	Risks for vertical services supporting URLLC in IMT-2020 private networks	6
9	Deployment scenarios of security functions for operation of vertical services supporting URLLC in IMT-2020 private networks	7
10	Security and monitoring requirements for operation of vertical services supporting URLLC in IMT-2020 private networks.....	9
	10.1 Security for NMSF	10
	10.2 Security for NMCF.....	11
	Annex A – NMSF characteristics	12
	Annex B – NMCF characteristics	14
	Annex C – Visualization of monitoring results	15
	Appendix I – Use cases of IMT-2020 private network for vertical services	17
	Bibliography.....	20

Recommendation ITU-T X.1813

Security and monitoring requirements for operation of vertical services supporting ultra-reliability and low-latency communication (URLLC) in IMT-2020 private networks

1 Scope

This Recommendation specifies the security requirements for the operation of vertical services supporting ultra-reliable and low-latency communications (URLLC) in IMT-2020 private networks. It identifies security threats and risks that arise when providing vertical services supporting URLLC in IMT-2020 private networks and describes security deployment scenarios of the IMT-2020 private networks for the operation of vertical services supporting URLLC.

In this Recommendation, monitoring of communication contents is out of scope for privacy protection purposes.

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 Y.3102] Recommendation ITU-T Y.3102 (2018), *Framework of the IMT-2020 network*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 5G non-public network [b-3GPP TS 22.261]: A 5G network that is intended for private use.

3.1.2 attack [b-ISO13491-1]: Attempt by an adversary on the device to obtain or modify sensitive information or a service they are not authorized to obtain or modify.

NOTE 1 – Network functions (NF) 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.

3.1.3 deployment [b-ISO/IEC/IEEE 24765]: Phase of a project in which a system is put into operation and cutover issues are resolved.

3.1.4 domain [b-ISO/IEC 14888-1]: Set of entities operating under a single security policy.

EXAMPLE – Public key certificates created by a single authority or by a set of authorities using the same security policy.

3.1.5 Internet of things (IoT) [b-ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

3.1.6 network monitoring [b-ISO/IEC 27033-1]: Process of continuously observing and reviewing data recorded on network activity and operations, including audit logs and alerts, and related analysis.

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

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

3.1.9 stakeholder [b-ISO/PAS 19450]: Individual, organization, or group of people that have an interest in, or might be affected by the system being contemplated, developed, or deployed.

3.1.10 trust [b-ISO/IEC 25010]: Degree to which a user or other stakeholder has confidence that a product or system will behave as intended.

3.1.11 vertical service [b-5G-PPP]: From a business perspective, a vertical service is a service focused on a specific industry or group of customers with specialized needs (e.g., automotive services, entertainment services, e-health services, industry 4.0).

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 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 the ITU-T context.

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

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

NOTE – The term relates to the development of 5G communication technology, where a community of stakeholders from industry and academia contribute their products, technology and expertise, to enable functionality at different layers of the 5G value stack e.g., infrastructure, network, platform, service, and application.

3.2.3 IMT-2020 private network: 5G non-public network (see clause 3.1.1) that utilizes both virtual and physical elements of an IMT-2020 communication system and is intended for the sole use of a private entity such as an enterprise.

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

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

5GC	5G Core
AMF	Access and Mobility Management Function
DDoS	Distributed Denial of Service
DPI	Deep Packet Inspection
EC	Edge Computing
EDR	Endpoint Detection and Response
GTP	GPRS Tunnelling Protocol

IoT	Internet of Things
MEC	Multi-access Edge Computing
MEC DP	MEC Data Plane
mMTC	massive Machine-Type Communications
NF	Network Function
NMCF	Network Monitoring Client Function
NMF	Network Monitoring Function
NMSF	Network Monitoring Server Function
NPN	Non-Public Network
PLMN	Public Land Mobile Network
RTT	Round Trip Time
SBA	Service-Based Architecture
SMF	Session Management Function
UDM	Unified Data Management
UE	User Equipment
UID	User ID
UPF	User Plane Function
URLLC	Ultra-Reliable and Low-Latency Communication

5 Conventions

This Recommendation uses the following conventions:

The keywords "**is required to**" indicate a requirement that 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 that 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 that 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 that 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

IMT-2020 system is architected to support network operators for data connectivity and services based on techniques such as network function virtualization and software defined networking. A service-based architecture (SBA) is defined by 3GPP [b-3GPP TS 23.501], whereby the control plane functionality and common data repositories of the IMT-2020 network are delivered by way of a set of interconnected network functions (NFs), each having the authorization to access each other's services. Figure 1 depicts the IMT-2020 system architecture.