

Recommendation

ITU-T X.1819 (09/2024)

SERIES X: Data networks, open system communications
and security

International Mobile Telecommunications (IMT) security

Security capabilities of network layer for IMT-2020/5G edge computing

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	X.1000-X.1099
SECURE APPLICATIONS AND SERVICES (I)	X.1100-X.1199
CYBERSPACE SECURITY	X.1200-X.1299
SECURE APPLICATIONS AND SERVICES (II)	X.1300-X.1499
CYBERSECURITY INFORMATION EXCHANGE	X.1500-X.1599
CLOUD COMPUTING SECURITY	X.1600-X.1699
QUANTUM COMMUNICATION	X.1700-X.1729
DATA SECURITY	X.1750-X.1799
INTERNATIONAL MOBILE TELECOMMUNICATIONS (IMT) SECURITY	X.1800-X.1839
METaverse AND DIGITAL TWIN SECURITY	X.2000-X.2199
SOFTWARE SUPPLY CHAIN SECURITY	X.2150-X.2199
ARTIFICIAL INTELLIGENCE (AI) / MACHINE LEARNING (ML) SECURITY	X.2200-X.2249

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

Recommendation ITU-T X.1819

Security capabilities of network layer for IMT-2020/5G edge computing

Summary

Recommendation ITU-T X.1819 describes the necessary security capabilities of the network layer for edge computing for the IMT-2020/5G network. Edge computing for international mobile telecommunications (IMT-2020)/5G networks (IMT-2020/5G EC) will play a key role in low latency services and traffic offload services in next generations of international mobile telecommunication (IMT) networks. Several prominent factors could increase the complexity and enlarge the security risks to the network layer that supports IMT-2020/5G EC and even bring new security challenges to network security operation. These factors include the flexible network architectures of IMT-2020/5G, the variable deployment positions of EC, various application scenarios, different types of customers' private networks and access networks, etc. The boundaries between the telecommunication networks and the private networks would be more ambiguous, and the exposure surface would be expanded. Therefore, security requirements and measures of the network layer including telecommunication networks and private networks should be specified.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.1819	2024-09-06	17	11.1002/1000/15892

Keywords

Edge computing, IMT-2020/5G, security capability, security requirement.

* To access the Recommendation, type the URL <https://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, and 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 2025

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	2
6 Introduction	3
6.1 Generic description of the network layer for IMT-2020/5G EC	3
6.2 Deployment scenarios	3
7 Security threats and requirements.....	4
7.1 Security threats	4
7.2 Security requirements	5
8 Security capabilities.....	6
8.1 Security protection capabilities	6
8.2 Security risk detection and analysis capabilities	14
8.3 Security incident response and recovery capabilities	15
Bibliography.....	17

Recommendation ITU-T X.1819

Security capabilities of network layer for IMT-2020/5G edge computing

1 Scope

This Recommendation describes the necessary security capabilities of the network layer for edge computing for the IMT-2020/5G network (IMT-2020/5G EC). It first outlines the network layer for IMT-2020/5G EC in general, and then describes the deployment scenarios in detail. It also identifies specific security threats and requirements arising from unique IMT-2020/5G EC features. Finally, to combat security threats, this Recommendation proposes various security capabilities for the network layer of IMT-2020/5G EC.

Conformance with this ITU-T Recommendation is not to be taken as any proof of evidence for claiming compliance with any national or regional law, regulation or policy. The technical, organizational, and procedural means described in this ITU-T Recommendation do not guarantee in any way the constitution of any level of security that may be put upon certain correspondence by specific national or regional law, regulation and policy.

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.1047] Recommendation ITU-T X.1047 (2021), *Security requirements and architecture for network slice management and orchestration*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [b-ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2 denial-of-service attack [b-ITU-T X.800]: The prevention of authorized access to resources or the delaying of time-critical operations.

3.1.3 distributed denial-of-service attack [b-ISO/IEC 27039]: 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 edge computing [b-ITU-T Y.3073]: This refers to a strategy to deploy processing capability at network edge where end terminals are connected, and to perform the processing of data which is derived from and fed to the end terminals.

3.1.5 virtual machine (VM) [b-ITU-T X.1603]: An efficient, isolated, logical duplicate of a real machine.

3.1.6 network slice [b-ITU-T Y.3074]: This is a complete end-to-end logically partitioned network providing dedicated telecommunication services and network capabilities. The behaviour of the network slice is realized via network slice instance(s).

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 edge computing for IMT-2020/5G (IMT-2020/5G EC): An implementation of edge computing at the edge of an IMT-2020/5G network.

3.2.2 network layer for IMT-2020/5G EC: A logical plane for routing and connection management that consists of IMT-2020/5G network elements and counterpart network entities, including IMT-2020/5G core network entities, servers, switches and routers of edge computing, and the counterpart routing or accessing entities in the private network.

3.2.3 edge computing migration: Migrating applications, data and other digital assets from one edge computing node to another edge computing node with little impact on the continuity of services.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACL	Access Control List
API	Application Open Interface
CN	Core Network
DDoS	Distributed Denial of Service
DMZ	Demilitarized Zone
DOS	Denial of Service
EC	Edge Computing
gNB	Next Generation NodeB
ID	Identifier
IMT-2020	International Mobile Telecommunications 2020
IMT-2020/5G	Fifth Generation mobile networks
IMT-2020/5G EC	Edge Computing for IMT-2020/5G network
IP	Internet Protocol
RAN	Radio Access Network
SMF	Session Management Function
UPF	User Plane Function
WAF	Web Application Firewall

5 Conventions

In this Recommendation:

The keyword "should" indicates a requirement which is recommended but which is not absolutely required. Thus, this requirement does not need to be present to claim conformance.

The keyword "could" indicates 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