

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1812

(05/2022)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

IMT-2020 Security

Security framework based on trust relationships for the IMT-2020 ecosystem

Recommendation ITU-T X.1812

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

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



Recommendation ITU-T X.1812

Security framework based on trust relationships for the IMT-2020 ecosystem

Summary

Recommendation ITU-T X.1812 identifies stakeholders in an International Mobile Telecommunications-2020 (IMT-2020; also known as fifth generation) ecosystem, analyses trust relationships amongst them, identifies threats and clarifies security responsibilities for each stakeholder, specifies security boundaries between stakeholders, and establishes a security framework based on these trust relationships.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1812	2022-05-20	17	11.1002/1000/14808

Keywords

Ecosystem, framework, IMT-2020, trust.

* 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	Security framework supported by the trusted model.....	5
8	Stakeholder role in scenarios for the IMT-2020 ecosystem	6
	8.1 General	6
	8.2 Scenario 1: Virtualization network deployment in a network operator domain	6
	8.3 Scenario 2: Interconnection and roaming.....	8
	8.4 Scenario 3: Car rental with remote operation.....	9
	8.5 Scenario 4: Network capability exposure for industry	10
	8.6 Scenario 5: Supply chains	12
	8.7 Stakeholders in the IMT-2020 ecosystem	13
9	Trust level, trust criteria, and trust model.....	14
	9.1 General	14
	9.2 Trust levels	15
	9.3 Trust criteria	17
	9.4 Trust model based on trust relationship mapping.....	18
10	Security requirements supported by trust model based on trust relationships.....	19
	10.1 General	19
	10.2 Security requirements from trust level	19
	10.3 Interpreting trust to detailed assurance requirements.....	22
	Bibliography.....	24

Introduction

The set of stakeholders in an International Mobile Telecommunications-2020 (IMT-2020; also known as fifth generation (5G)) system is larger and more varied than in previous communication systems. In the second, third and fourth generation (2G, 3G and 4G), the main stakeholders can be summarized as service providers, network operators, equipment vendors and subscribers. However, in an IMT-2020 ecosystem, vertical players are also involved, such as industrial and commercial enterprises. Also, service providers can be sub-divided into cloud platform operators, data analyst companies, application providers, etc. Furthermore, at the terminal end, subscribers are not only end users as was the case previously. Subscribers can include a range of different types of stakeholder, especially for commercial terminals, e.g., in the shared vehicle communication use case. These changes create complex relationships among various stakeholders and raise a series of new security issues for IMT-2020 ecosystems.

The IMT-2020 network also introduces new features. For example, the introduction of network virtualization in IMT-2020 breaks the fixed connections between network entities and enables software-defined networks. Another example is provided by service-based architecture. With such architecture, more cloud-related features could be built into an IMT-2020 network. Also, slicing can enable more effective co-operation between an IMT-2020 network and services.

As time goes on, increasing numbers of information technology (IT) techniques will be applied to IMT-2020 systems, not only to their services, but also their network. The IMT-2020 network is entirely based on the Internet protocol. Its architecture specification is based on services rather than reference points, as was the case for previous network architectures. Signals are increasingly transferred from the Internet rather than dedicated networks. The transport protocol in IMT-2020 networks is changed from diameter [b-IETF RFC 6733], which is less popular than the hypertext transfer protocol that is widely used globally. All these changes will bring benefits for the IMT-2020 network and service deployment and operation.

However, the use of popular protocols and an open connection environment could also bring benefits to attackers. An attacker will not need to spend that much time studying complex telecommunication protocols, and it will potentially be simpler to find an intrusion point in a network. As a result, in IMT-2020 networks it is not reasonable to assume that internal communication is trustworthy anymore. Thus, the changes from 4G to IMT-2020 break the trust relationship between network operators.

Additionally, the IMT-2020 network is designed to be more flexible in order to meet the varied service requirements. In particular, slicing has been introduced into IMT-2020 networks. IMT-2020 networks can also expose some capabilities to services. Such capability exposure will enable an IMT-2020 service to control some network functions. These new features will make the security boundary between the IMT-2020 network and services more ambiguous.

This Recommendation identifies stakeholders in an IMT-2020 ecosystem, analyses trust relationships among them, identifies threats and clarifies security responsibilities for each stakeholder, specifies security boundaries between stakeholders and establishes a security framework based on these trust relationships.

Recommendation ITU-T X.1812

Security framework based on trust relationships for the IMT-2020 ecosystem

1 Scope

This Recommendation specifies a security framework based on trust relationships for an International Mobile Telecommunications-2020 (IMT-2020) ecosystem. This Recommendation describes a general approach to the:

- identification of scenarios for providing IMT-2020 services;
- identification of stakeholders in an IMT-2020 ecosystem;
- analysis of trust relationships among stakeholders;
- identification of threats applying to each stakeholder;
- clarification of security responsibilities for each stakeholder;
- specification of security boundaries between stakeholders;
- specification of security requirements based on trust model; and
- establishment of a security framework based on the trust relationships between stakeholders.

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.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 business unit [b-ISO/TS 21089]: Discrete and accountable function or sub-function within an organization

NOTE – A business unit can include a department, service or specialty within a healthcare provider organization.

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

3.1.3 developer [b-NIST SP 800-53]: An entity that includes: (i) developers or manufacturers of information systems, system components, or information system services; (ii) systems integrators; (iii) vendors; and (iv) product resellers.

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

3.1.6 lifecycle [b-ISO/IEC/IEEE 15288]: Evolution of a system, product, service, project or other human-made entity, from conception through retirement.

3.1.7 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.

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

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

3.1.10 system development [b-ISO/IEC 2382]: Process that usually includes requirements analysis, system design, implementation, documentation and quality assurance.

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

3.1.12 trust level [b-ISO 28598-1]: Customer's estimate of the weight of prior, supplementary and indirect evidence of the supplier's capability to fulfil the specified quality requirements.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 external service provider: A set of entities that includes: a) entities within the organization but outside the security authorization boundaries established for organizational information systems; b) entities outside the organization either in the public sector (e.g., federal agencies) or private sector (e.g., commercial service providers); or c) some combination of the public and private sector options.

NOTE – Adapted from [b-NIST SP 800-53].

3.2.2 supply chain: A network of organizations that are involved, through upstream and downstream linkages, in the processes and activities that produce value in the form of products and services in the hands of the ultimate consumer.

3.2.3 system development lifecycle: A structured approach to planning, creating, testing, deploying and maintaining an information system.

3.2.4 trust model: Model that consists of components that describe the trust relationships and chains between stakeholders.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

2G	second Generation
3G	third Generation
4G	fourth Generation
5G	fifth Generation
5GC	fifth Generation Core
BS	Base Station

CAB	Conformity Assessment Body
E2E	End to End
HO	Home Operator
ICP	Internet Content Provider
ICT	Information and Communication Technology
IMT-2020	International Mobile Telecommunications-2020
IoT	Internet of Things
IoV	Internet of Vehicles
IPX	Internetwork Packet exchange
ISP	Internet Service Provider
IT	Information Technology
NE	Network Element
NESAS	Network Equipment Security Assurance Scheme
NF	Network Function
NFV	Network Function Virtualization
NPN	Non-Public Network
PII	Personally Identifiable Information
PLMN	Public Land Mobile Network
SCAS	Security Assurance Specification
SDL	Security Development Lifecycle
UICC	Universal Integrated Circuit Card
VNF	Virtualized Network Function
VO	Visited Operator

5 Conventions

In this Recommendation:

The phrase "**is recommended**" indicates a requirement that is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformity.

The phrase "**can optionally**" indicates 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 or service provider. Rather, it means the vendor may optionally provide the feature and still claim conformity with this Recommendation.

6 Overview

Before the 5G era, telecommunication systems were mainly used for providing telephony, Internet access and related services. As a result of the capability and rate constraints of these systems, the use cases were simple in general. In particular, only a small number of roles was involved in a communication system. For the call service, the players involved are the caller, the callee and the mobile network. For the data service, the players are the terminal, the mobile network and service or application providers. In addition, in order to support the building of networks and application

systems, vendors are involved. Terminal manufacturers and universal integrated circuit card (UICC) providers are relevant at the terminal. These are the main roles involved in 2G, 3G and 4G telecommunication systems.

However, in the IMT-2020 ecosystem, things are different. The ecosystem does not only contain all stakeholders in telecommunication system in terminal, network and service, but also other stakeholders. At the terminal, subscribers are not only end users, as was the case before, because the mobile device could be one of many different types of equipment that may be shared between multiple parties, not just a telephone. In the network, IMT-2020 introduces a range of new features. For example, network virtualization in IMT-2020 breaks the fixed connection between network entities and enables software-defined networks that break the security border of network deployment. More and more information technology (IT) techniques are applied in IMT-2020 networks that can also be exploited by attackers. The network exposure service opens interfaces in the control plane rather than the user plane for an attacker. For services, vertical players are involved, such as industrial and commercial enterprises. This divides service providers into cloud platform operators, data analyst companies, application providers, etc., as shown in Figure 1.

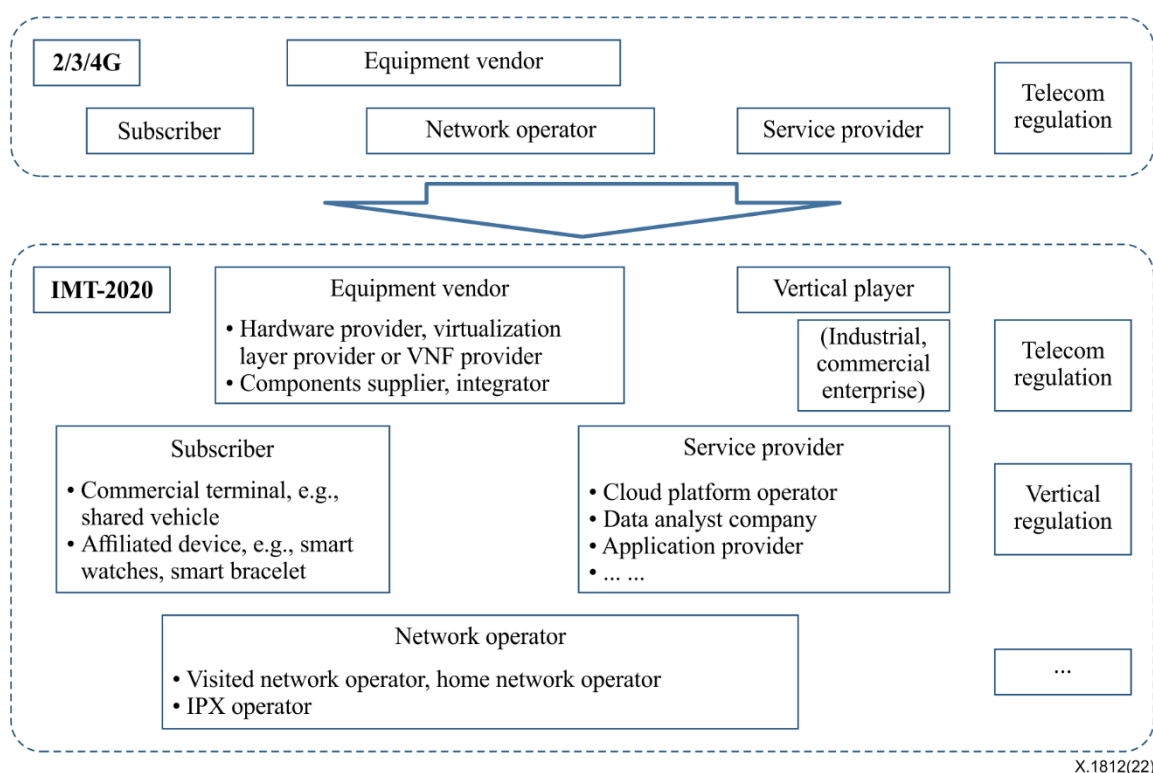


Figure 1 – Ecosystem evolution from 2G, 3G, 4G to IMT-2020

In this case, the trust relationship of the IMT-2020 system is different. Users or subscribers and network or service systems are much closer than before. The complex and long-tailed supply chain pushes operators to consider more about the evaluation of suppliers. The tight bond between service and network makes vertical industries rely heavily on the network and requires more strict trust and security. Provision of a new trust model for the IMT-2020 ecosystem needs consideration, to formulate a clear security requirement and security boundary between stakeholders. In this way, communication efficiency can be improved as much as possible with assurance of data security.

Five properties, namely resilience, communication security, identity management, personally identifiable information (PII) protection and security assurance, impact the trustworthiness of an IMT-2020 system.

- **Resilience:** Resilience is the capability of an organization to resist being affected by disruptions. A variety of complementary and partially overlapping features in IMT-2020 can help achieve resilience of an IMT-2020 system to cyberattacks and non-malicious incidents.
- **Communication security:** Communication security is applied to data communication in IMT-2020. Secure communication for devices and for its own infrastructure is vital in an IMT-2020 system.
- **Identity management:** An identity management system consists of processes and policies involved in managing the lifecycle, value, type and optional metadata of attributes making up identities of entities in an IMT-2020 system. Provision of secure identity management for identification and authentication of subscribers, roaming or not, and ensuring that only genuine subscribers can access network services is recommended. Such systems are built on strong cryptographic primitives and security characteristics.
- **PII protection:** Data privacy is defined in [b-ISO/TS 21719-2] as the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal information. PII protection involves protecting PII that can be used by unauthorized parties to identify subscribers.
- **Security assurance:** Security assurance provides grounds for justified confidence that a claim about meeting security objectives has been or will be achieved. Security assurance is a means to ensure that network equipment meets security requirements and is achieved through the adoption of secure development and product lifecycle processes.

7 Security framework supported by the trusted model

This Recommendation analyses and determines the roles of stakeholders in the IMT-2020 ecosystem and the trust relationship between roles by analysing several typical scenarios. It then tries to determine the level of trust with the key factors to be considered. On this basis, it gives recommendations on how to determine security requirements based on the trust level, and to form a security framework based on trust relationship, as shown in Figure 2.

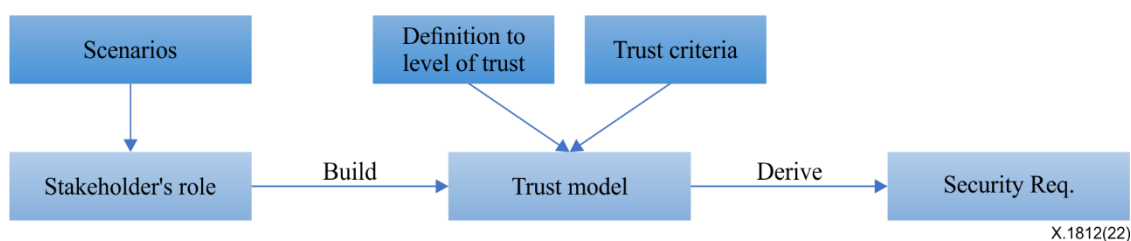


Figure 2 – Way forward to build security framework based on trust relationships for IMT-2020 ecosystem

Based on the role and relationship, trust model and security requirements of all stakeholders, a security framework supported by the trust model established in this Recommendation is illustrated in Figure 3. All components in the framework are described in: clause 8 for the stakeholders' role; clause 9 for the trust model; and clause 10 for security requirements.