International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1604

(03/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cloud computing security – Cloud computing security design

Security requirements of Network as a Service (NaaS) in cloud computing

Recommendation ITU-T X.1604

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	X.1700–X.1729

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

Recommendation ITU-T X.1604

Security requirements of Network as a Service (NaaS) in cloud computing

Summary

Recommendation ITU-T X.1604 analyses security threats and challenges on Network as a Service (NaaS) in cloud computing and specifies security requirements of NaaS in NaaS application, NaaS platform and NaaS connectivity aspects based on corresponding cloud capability types.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1604	2020-03-26	17	11.1002/1000/14093

Keywords

Cloud, Network as a Service, security requirements.

* 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, 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 TSB patent database at http://www.itu.int/ITU-T/ipr/.

© ITU 2020

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	Overview	3
7	Security threats and challenges of Network as a Service in cloud computing	4
	7.1 Security threats and challenges of NaaS application	4
	7.2 Security threats and challenges of NaaS platform	4
	7.3 Security threats and challenges of NaaS connectivity	5
8	Security requirements for NaaS application	5
	8.1 Security requirements for NaaS application	5
	8.2 Security requirements for NaaS platform	6
	8.3 Security requirements for NaaS connectivity	7
Bibliography		8

Recommendation ITU-T X.1604

Security requirements of Network as a Service (NaaS) in cloud computing

1 Scope

This Recommendation analyses security threats and challenges on Network as a Service (NaaS) in cloud computing, and specifies security requirements of NaaS in NaaS application, NaaS platform and NaaS connectivity aspects based on corresponding cloud capability types.

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.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and Vocabulary.*

[ITU-T Y.3512] Recommendation ITU-T Y.3512 (2014), *Cloud computing – Functional requirements of Network as a Service.*

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 authentication [b-ISO/IEC 18014-2]: Provision of assurance in the identity of an entity.

3.1.3 authorization [b-ITU-T X.1251]: The authorization service is designed to make decisions regarding the user's access rights and enforce authorization decisions according to the user's privileges. Authorization is an optional service; it is only provided when access to resources needs to be controlled based on the user's rights.

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

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

3.1.6 firewall [b-ISO/IEC 27033-1]: Type of security barrier placed between network environments – consisting of a dedicated device or a composite of several components and techniques – through which all traffic from one network environment traverses to another, and vice versa, and only authorized traffic, as defined by the local security policy, is allowed to pass.

3.1.7 intrusion detection system [b-ISO/IEC 27039]: Information systems used to identify that an intrusion has been attempted, is occurring, or has occurred.

3.1.8 key [b-ITU-T X.800]: A sequence of symbols that controls the operations of encipherment and decipherment.

3.1.9 key management [b-ITU-T X.800]: The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

3.1.10 public-key certificate (PKC) [b-ITU-T X.509]: The public key of an entity, together with some other information, rendered unforgeable by digital signature with the private key of the certification authority (CA) that issued it.

3.1.11 threat [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which may result in harm to a system or organization.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BoD	Bandwidth on Demand
CSC	Cloud Service Customer
CSP	Cloud Service Provider
DDoS	Distributed Denial of Service
DoS	Denial of Service
NaaS	Network as a Service
SNMP	Simple Network Management Protocol
vCDN	virtual Content Delivery Network
vEPC	virtualized Evolved Packet Core
vFW	virtual Firewall
VPN	Virtual Private Network

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

According to [ITU-T Y.3500], a cloud service category is a group of cloud services that proposes a common set of quantities. Network as a Service (NaaS) is one of the cloud service categories in which the capability provided to the cloud service customer (CSC) is transport connectivity and any related network capabilities.

As defined in [ITU-T Y.3512], NaaS services can provide any of the following three cloud capabilities: NaaS application service, NaaS platform service and NaaS connectivity service.

- **NaaS application service** provides a CSC cloud network application such as virtual router, virtual content delivery network (vCDN), virtualized evolved packet core (vEPC) and virtual firewall (vFW).
- **NaaS platform service** provides a CSC network platform that offers a programmable environment for network functionalities.
- **NaaS connectivity service** provides CSC provisioning and uses networking connectivity resources such as flexible and extended virtual private network (VPN), bandwidth on demand (BoD), etc.

The high-level concept of NaaS can be described as shown in Figure 1.

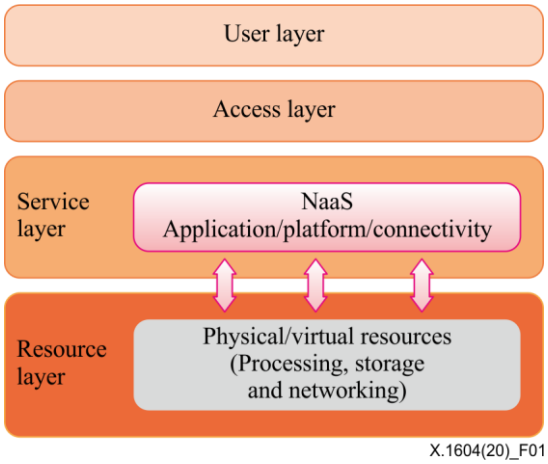

Figure 1 – High-level concept of NaaS

By using these three kinds of networking services, NaaS can provide network functions in cloud computing including: coordination of compute and storage virtualization with network capabilities, harmonized control of heterogeneous network technologies and on-demand reconfiguration.

On the other hand, NaaS also faces several security challenges:

- **Security threats and challenges on NaaS application**: A NaaS application service is to provide virtual network applications to CSC by CSP, such as virtual firewall (vFW), virtual router, virtual delivery network (vCDN), etc. A NaaS application service faces security challenges on application security vulnerabilities, security risks of network virtualization, shared use of physical network devices, etc.
- **Security threats and challenges on NaaS platform**: A NaaS platform service is to provide software environments and a platform to manage, deploy and run network applications to CSC by the CSP. Security challenges on NaaS platform includes, but are not limited to, DoS attacks on network platforms, security vulnerabilities of operating systems, broken access control, etc.
- **Security threats and challenges on NaaS connectivity**: A NaaS connectivity service is to provide network connection to CSC by the CSP, such as virtual private network (VPN),

bandwidth on demand (BoD), etc. A security problem of the connectivity service causes risks not only to the NaaS services, but also to other cloud resources and to data of the CSC. Security challenges on NaaS connectivity service includes, but are not limited to, eavesdropping, man in the middle attack, etc.

This Recommendation analyses security requirements for NaaS in cloud computing, including NaaS application, NaaS platform and NaaS connectivity.

7 Security threats and challenges of Network as a Service in cloud computing

Clauses 7 and 8 in [ITU-T X.1601] document security threats and challenges for CSC and CSP in cloud computing respectively. NaaS in cloud also faces similar security threats and challenges to those defined in [ITU-T X.1601] as shown below:

a) system vulnerabilities;

b) data loss and leakage;

c) insecure service access;

d) unauthorized administration access;

e) insider threats;

f) loss of trust;

g) loss of governance;

h) loss of confidentiality;

i) service unavailability; and

j) shared environment.

For each cloud capability, NaaS in cloud computing faces particular security threats and challenges.

7.1 Security threats and challenges of NaaS application

a) Network and system vulnerabilities: Potential security vulnerabilities of NaaS application could be exploited by attackers. Technical defects of NaaS application virtualization could cause several security risks; in addition, immature operation and maintenance technology could result in risks being more serious.

b) Shared use of physical network devices: As physical network devices are shared, data on one shared device could be lost, leaked or misused.

c) Insecure access: Insecure access to NaaS application could cause application data to be lost, leaked or misused.

d) Unauthorized administration access: Unauthorized administration access to the NaaS application could result in data loss.

e) Application unavailability: A NaaS application can be attacked by a denial of service (DoS) or distributed denial of service (DDoS) attack; in addition, the attack could cause hardware equipment to be damaged and cause data loss or destruction.

7.2 Security threats and challenges of NaaS platform

a) DoS attacks on network platform: When one or more platforms have been subjected to denial of service (DoS) attacks, the platform and other virtualized platforms cannot respond because of CPU and memory transition consumption.

b) Security vulnerabilities of operating system: Data on NaaS platforms could be lost; in addition, security vulnerabilities of operating systems could cause viruses to spread and other serious security risks.

c) Broken access control: Broken access control could cause data to be lost, leaked or misused.

d) Network platform unavailability: Unavailability of a NaaS platform could result in unavailability of NaaS services, so related NaaS applications and NaaS connectivity may not work as well.

e) Unauthorized administration access: Unauthorized administration access to the NaaS platform could result in data to be lost, leaked or misused. For example, attackers may use a system vulnerability to gain unauthorized administration access to the NaaS platform and modify the data collection destination IP address to that of the attacker's.

f) Insider employee threats: If a NaaS service's customer is a company or organization, not a person, the organization’s employees share the "administration" passwords, and so does the NaaS service provider. Careless or inadequately trained users (or family members in a consumer setting), or malicious action by disgruntled employees will always pose a significant threat.

7.3 Security threats and challenges of NaaS connectivity

a) Eavesdropping: Connection data and transmission data could be subject to eavesdropping by attackers.

b) Network connection attack: Network attacks may occur during network connection, such as man in the middle attacks, DoS attacks, etc.

c) Data loss and leakage: When using NaaS services, NaaS customers usually use the network provided by NaaS providers to transport data. This data may involve personal privacy, trade secrets and political issues. So data leakage is a serious threat to NaaS users.

d) Spoofing: Attackers could masquerade as the management system, or data storage server of a NaaS of cloud computing, and this can cause the loss of connection or transmission data.

e) Tampering and intercepting: Damaged network equipment, hacker intrusion and bankruptcy of a NaaS service provider are likely to cause data loss that cannot be recovered. In addition, hackers can also tamper with data if they successfully enter the network.

f) Insecure network access: Insecure network access could cause connection or transmission data to be lost, leaked or misused.

g) Insecure identity authentication: Insecure identity authentication could result in connection or transmission data to be lost, leaked or misused.

h) Network unavailability: The NaaS connectivity network could be attacked by a DoS or DDoS attack; in addition, DoS or DDoS attacks could cause servers of NaaS in cloud computing to crash.

i) Acquisition interface vulnerability: Attackers may use a monitoring data acquisition to exploit interface vulnerabilities.

j) Unauthorized administration access: Unauthorized administration access to a NaaS connectivity system could result in transmission data loss.

8 Security requirements for NaaS application

This clause identifies the security requirements for NaaS of cloud computing.

8.1 Security requirements for NaaS application

The security requirements for NaaS application include the following:

a) It is required to maintain integrity and accuracy of NaaS application data.

b) It is recommended to provide access control methods to NaaS application data such as white lists, black lists, etc.;

c) It is recommended that the CSP provides the appropriate access control methods to the CSC, such as white/black list, account and password, etc., to prevent unauthorized users from accessing systems or data. The common access control solutions for cloud computing are in [ITU-T X.1601].

d) It is required that the CSP supports the logging and auditing of NaaS application usage.

e) it is required that the CSP supports defences against the vulnerabilities of the NaaS application system; for example, the CSP could use penetration testing methods to prevent vulnerabilities of the NaaS application system.

f) It is required that the CSP provides backup methods to prevent NaaS application data loss, such as back up using physical disks, distributed data storage methods, etc. Common back up methods are described in [ITU-T X.1601].

Table 8-1 provides a summary mapping of NaaS application security threats to security requirements.

Table 8-1 – NaaS application: Security threats mapping to security requirements

Security threats	Security requirements
Application security vulnerabilities	b), d), e), f)
Security risks of network virtualization	a), b), c), d), f)
Shared use of physical network devices	a), b), c), d), f)
Insecure access	b), c), d), e), f)
Unauthorized administration access	b), c), d), f)
Application unavailability	d), e), f)

8.2 Security requirements for NaaS platform

The security requirements for a NaaS platform include the following:

a) It is required to maintain integrity and accuracy of NaaS platform data.

b) It is recommended to provide access control methods to NaaS platform data such as white lists, black lists, etc.

c) It is recommended that the CSP provides the appropriate access control methods to the CSC, such as white/black list, account and password, etc., to prevent unauthorized users from accessing systems or data. The common access control solutions for cloud computing are described in [ITU-T X.1601].

d) It is required that the CSP supports the logging and auditing of NaaS platform usage.

e) It is required that the CSP implements defences against the vulnerabilities of the NaaS platform system; for example, the CSP should prevent data loss and leakage on the NaaS platform.

f) It is required that the CSP provides backup methods to prevent NaaS platform data loss, such as back up using physical disks, distributed data storage methods, etc. Common back up methods are described in [ITU-T X.1601].

Table 8-2 provides a summary mapping of NaaS platform security threats to security requirements.

Table 8-2 – NaaS platform: security threats mapping to security requirements

Security threats	Security requirements
DoS attacks on network platform	a), b), c), d), e), f)
Security vulnerabilities of operating system	a), b), d), e), f)
Broken access control	a), b), c), d), e), f)
Network platform unavailability	a), d), e), f)
Unauthorized administration access	b), c), d), f)
Insider employees threats	b), d), f)

8.3 Security requirements for NaaS connectivity

The security requirements for NaaS connectivity include the following:

a) It is required to maintain integrity and accuracy of NaaS connectivity data.

b) It is recommended to provide access control methods to the interfaces of NaaS connectivity such as white lists, black lists, etc.

c) It is recommended to provide cryptographic methods to ensure the security of the connection and transmission data.

d) It is recommended to use standard network protocols between the cloud resources and NaaS connectivity servers, such as Simple Network Management Protocol (SNMP) or other standard network protocols.

e) It is recommended that the CSP provides the appropriate access control methods to the CSC, such as white/black list, account and password, etc, to prevent unauthorized users from accessing systems or data. The common access control solutions for cloud computing are in [b-ITU-T X.1601].

f) It is required that the CSP supports the logging and auditing of NaaS connectivity usage.

g) It is required that the CSP implements authentication methods to protect access to the NaaS connectivity data, such as two-factor authentication or other methods. Common authentication methods for cloud computing are described in [ITU-T X.1601].

h) It is required that the CSP supports defences against the vulnerabilities of the NaaS connectivity system. For example, the CSP could use penetration testing methods to prevent vulnerabilities of the NaaS connectivity system.

Table 8-3 provides a summary mapping of NaaS platform security threats to security requirements.

Table 8-3 – NaaS connectivity: security threats mapping to security requirements

Security threats	Security requirements
Eavesdropping	b), c), d), e), f), g) h)
Network connection attack	d), f), h)
Data loss and leakage	a), b), c), d), e), f), g) h)
Spoofing	a), b), d), e), f), g) h)
Tampering and intercepting	a), b), c), d), e), f), g) h)
Insecure network access	b), c), d), e), f), g) h)
Insecure identity authentication	b), c) , e), f), g) h)
Network unavailability	d), f), h)
Acquisition interface vulnerability	a), b), c), d), f), h)
Unauthorized administration access	c), f), g)

Bibliography

[b-ITU-T E.409] Recommendation ITU-T E.409 (2004), *Incident organization and security incident handling: Guidelines for telecommunication organizations*.

[b-ITU-T X.509] Recommendation ITU-T X.509 (2019) | ISO/IEC 9594-8:2020, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991) | ISO/IEC 7498-2:1989, *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.810] Recommendation ITU-T X.810 | ISO/IEC 10181-1 :1995, *Information technology – Open System Interconnection – Security frameworks for open systems: Overview*.

[b-ITU-T X.1251] Recommendation ITU-T X.1251 (2019), *Use cases for structured threat information expression*.

[b-ITU-T Y.3502] Recommendation ITU-T Y.3502 | ISO/IEC 17789:2014, *Information technology – Cloud computing – Reference architecture*.

[b-ISO/IEC 18014-2] ISO/IEC 18014-2:2009, *Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens*.

[b-ISO/IEC 19440] ISO/IEC 19440:2007, *Enterprise integration – Constructs for enterprise modelling*.

[b-ISO/IEC 19944] ISO/IEC 19944:2017, *Information technology – Cloud services and devices: data flow, data categories and data use*.

[b-ISO/IEC 20000-1] ISO/IEC 20000-1:2011, *Information technology – Service management – Part 1: Service management system requirements.*

[b-ISO/IEC 27000] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27033-1] ISO/IEC 27033-1:2015, *Information technology – Security techniques – Network security – Part 1: Overview and concepts*.

[b-ISO/IEC 27039] ISO/IEC 27039:2015, *Information technology – Security techniques – Selection, deployment and operations of intrusion detection and prevention systems (IDPS).*

[b-ISO/IEC 27729] ISO/IEC 27729:2012, *Information and documentation – International standard name identifier (ISNI).*

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020