International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1452

(10/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Security protocols (2)

Guidelines for security services provided by operators

Recommendation ITU-T X.1452

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	
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
5G SECURITY	X.1800–X.1819

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

Recommendation ITU-T X.1452

Guidelines for security services provided by operators

Summary

Recommendation ITU-T X.1452 classifies potential use cases of security services provided by operators and analyse specific requirements for security services, thus providing guidelines for operators to safeguard and improve their security services.

Due to the growing number of innovations in services in network and telecommunication domains, operators face a pressing need to explore new services based on their network and services capabilities. In this transformation, operators have not only accumulated new assets and experiences with technologies and services for network and telecommunication, but also the capability of offering security services based on the full extent of their network and infrastructure deployments and operations. The specific nature of this class of services makes them exhibit a number of differences with more traditional telecommunication services (e.g., phone call, short message or mobile network access). In this context, the portfolio of security services that are currently in production and explored by operators need specific integration with the resources and assets of the telecommunication network and infrastructure; the risk level of this portfolio is actually higher should the security service itself be compromised as it is precisely supposed to turn the operator offering it into a security provider for end market customers. A compromise of the service will result in loss of trust by customers and will affect the whole range of services offered by the operator and will significantly increase the overall churn level, and customer dissatisfaction and disloyalty. Therefore, security assurance, defined as the degree of confidence reached in the security service, needs to be studied thoroughly. In order to offer a technical reference for operators and to guarantee security, security service guidelines provided by the operator need to be analysed and established.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1452	2020-10-29	17	11.1002/1000/14451

Keywords

Guidelines, operator, security services.

---

* 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/.

Table of Contents

Recommendation ITU-T X.1452

Guidelines for security services provided by operators

1 Scope

This Recommendation classifies potential use cases of security services provided by operators, analyses their specific requirements and specifies guidelines for operators to safeguard and improve their security services.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 collaboration agreement: A contract between two or more business organizations that results from the first step of the onboarding process and that specifies all onboarding parameters between the business organizations.

3.2.2 non-technical onboarding process: The non-technical steps, for legal, compliancy, risk, financial and sales support, for the integration of security services from a third party security service provider and relevant parties into the operator, specifying all parameters. including roles and responsibilities.

3.2.3 onboarding process: The steps taken to establish a collaboration agreement followed by the necessary technical and non-technical onboarding process steps, which integrate (e.g., merge the security services into one) a given security service from one business organization into another.

3.2.4 secure portable wireless access point (SPWAP): A portable device with a connecting function that transports traffic and data from a terminal to the Internet or intranet, together with security analysis and security filtering functions, such as analysing and filtering malicious uniform resource locators (URLs) or phishing websites. It is preconfigured with a subscriber identification module (SIM) card. It is similar to a mobile wireless local area network (WLAN) hotspot device.

3.2.5 security mechanism: A technical method to ensure security compliance of the security service being onboarded for both the third-party service provider and the relevant parties, as well as the operator.

3.2.6 security service: A service offering value to end customers based on security functionalities.

3.2.7 security service customer: A human being, organization, or system that uses a security service provided by operators.

3.2.8 security service provider: A business organization offering a portfolio of services based on security functionalities to end customers.

3.2.9 technical onboarding process: The technical steps for the pre-deployment, pre-configuration and security mechanisms of the security services to be integrated from a third-party security service provider and relevant parties into the operator.

3.2.10 third party security service provider: A given security service provider offering a security service to be onboarded by an operator.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

APN Access Point Name

CPSC Cloud Platform of Security Capabilities

CT Communication Technology

IP Internet Protocol

IT Information Technology

SIM Subscriber Identification Module

SPWAP Secure Portable Wireless Access Point

UE User Equipment

URL Uniform Resource Locator

USIM Universal Subscriber Identity Module

VPDN Virtual Private Dial-up Network

VPN Virtual Private Network

WLAN Wireless Local Area Network

5 Conventions

In this Recommendation:

The phrase "is required" indicates a requirement that must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

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 conformance.

In this Recommendation, the keywords "shall" and "should" may sometimes appear, in which case they are to be interpreted as “is required to” and “is recommended” respectively.

6 Overview of security services provided by operators

Due to the growing number of innovations in services in network and telecommunication domains, operators face a pressing need to explore new services based on their network and service capabilities.

In this transformation, operators have not only accumulated new assets and experiences with technologies and services for networks and telecommunications, but also the capability of offering security services based on the full extent of their network and infrastructure deployments and operations.

The specific nature of this class of services makes them exhibit a number of differences with the more traditional telecommunication services (e.g., phone calls, short messages or mobile network access). In this context, see the following.

– The portfolio of security services that are currently in production and explored by operators need specific integration with the resources and assets of telecommunication networks and infrastructure.

– The risk level on this portfolio is higher, should the security service itself be compromised. The security service is to be offered by an operator as a security provider to their end user. A compromise of such service will result in a loss of trust by end users. This loss of trust will span the whole range of services offered by the operator and will significantly damage end-user satisfaction and loyalty, thus increase the overall churn level.

7 Typical use cases

7.1 Secure connecting service

7.1.1 Customer

The customer of a secure connecting service provided by operators is an enterprise customer. This service aims to protect the enterprise customer by guaranteeing the security of the mobile office through secure access to the Internet and intranet of the enterprise.

7.1.2 Technical onboarding

1) Pre-deployment

The onboarding of a secure connecting service includes two main parts: a SPWAP and a cloud platform of security capabilities (CPSC). The secure connecting service can provide functions such as internet access, malicious website filtering, link selection and remote device monitoring.

Figure 7-1 illustrates onboarding of secure connecting services.

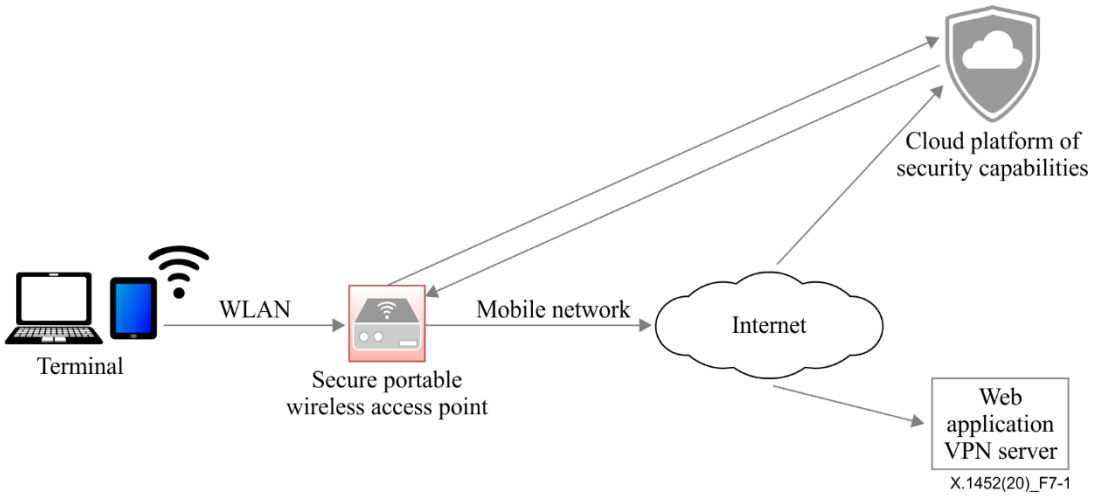

Figure 7-1 – Technical onboarding of secure connecting service

In Figure 7-1, the SPWAP is a portable device with security analysis and security filtering functions, which has been preconfigured with a SIM or universal subscriber identity module (USIM) card. It can be similar to a mobile WLAN hotspot device. The terminal can access the SPWAP by WLAN. The SPWAP is used as a network access point for connecting to the Internet or intranet of the enterprise through a mobile network. To connect to the Internet, the SPWAP will take advantage of various URL feature libraries on the CPSC to check the customer's accessing website or URL by access control, and then block the malicious URL or phishing website. To connect to the intranet of the enterprise, the SPWAP will make use of various link selection modes to access the intranet securely, such as access point name (APN), virtual private network (VPN) and virtual private dial-up network (VPDN).

The CPSC provides the security capabilities on the cloud and the ability to configure devices connected to it, such as recognizing malicious websites and managing resources. The SPWAP can query the CPSC, which shall respond. The CPSC can help the SPWAP to hold up malicious URLs or

phishing websites, as well as querying them in real time. The CPSC provides enterprise customers with a customer interface combining website blacklist configuration and customer information maintenance, etc. functions.

2) Collaboration among the operator and the relevant parties

In the secure connecting service, the entities include the terminal, the SPWAP, the CPSC and the web application VPN server. Accordingly, the mapping between the entities and the relevant parties is illustrated in Figure 7-1. In Table 1, the symbol "✓" indicates that the entity is related to a particular relevant party.

Table 1 – The mapping between the entities and the relevant parties

Entity	Relevant party		
	Customer	**Operator**	**Third party security service provider**
Terminal	✓		
SPWAP		✓	
CPSC		✓	
Web application VPN server			✓

The collaboration agreement should be pre-established between the operator and the web application VPN server. The collaboration agreement should include, but is not limited to:

1. clarification of the roles of each entity during service provision;
2. clarification of the responsibilities of each entity during service provision;
3. implementation support, to clarify the necessary support (e.g., functionality feature, supporting system and security solution) of each entity during service provision.

3) Security mechanisms

The security mechanisms (details can be seen in clause 10) in secure connecting service should include, but are not limited to:

1. authentication;
2. access control;
3. blacklist mechanism;
4. audit.

7.1.3 Process

There are five steps in the process of a secure connecting service, as illustrated in Figure 7-2.

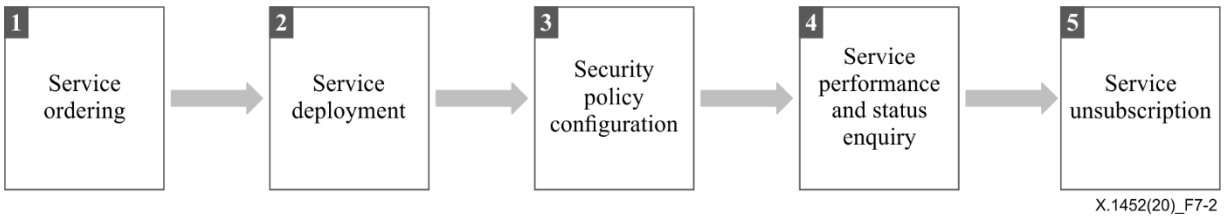

Figure 7-2 – Process of a secure connecting service

According to Figure 7-2, the process of a secure connecting service is as follows.

Step 1: Service ordering

1. The customer orders a secure connecting service.

Step 2: Service deployment

1. The account manager opens an account for the customer ordering a secure connecting service.
2. The account manager inserts the SIM or USIM card in the SPWAP.
3. The account manager delivers the SPWAP to the customer.
4. The customer activates the SPWAP.
5. The customer connects their end points to the SPWAP by WLAN hotspot.

Step 3: Security policy configuration

1. The manager of the SPWAP logs into the CPSC and configures the security policy.

Step 4: Service performance and status enquiry

1. The customer uses the service normally.
2. The customer can enquire about service status through the CPSC.

Step 5: Service unsubscription

1. If the customer no longer requires the secure connecting service, the customer can unsubscribe from it.

7.2 Abnormal flow cleaning service

7.2.1 Customer

The customer of an abnormal flow cleaning service provided by an operator is an enterprise customer. This service aims to protect the enterprise customer business from distributed denial-of-service attacks.

7.2.2 Technical onboarding

1) Pre-deployment

The onboarding of abnormal flow cleaning services includes three main components for: abnormal flow detection; abnormal flow cleaning; and service management. The abnormal flow cleaning service can provide functions such as abnormal flow detection, abnormal flow cleaning, flow logs analysis and report of attack event analysis.

Figure 7-3 illustrates the onboarding of an abnormal flow cleaning service.

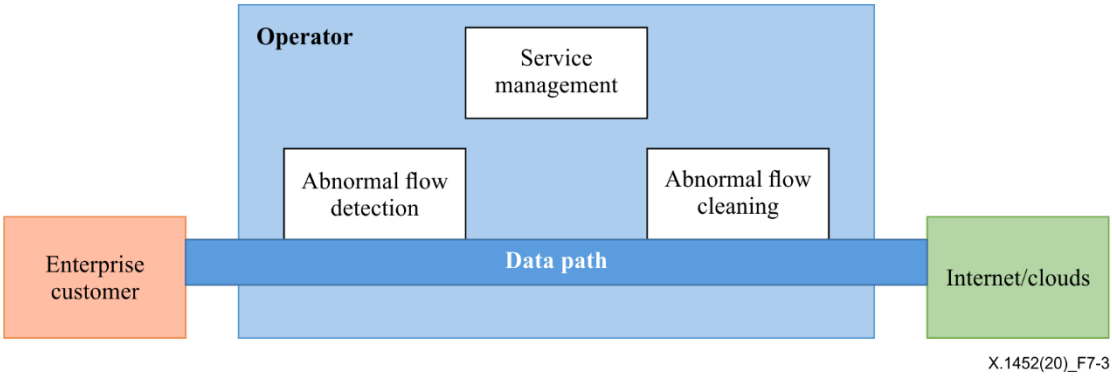

Figure 7-3 – Technical onboarding of abnormal flow cleaning service

The abnormal flow detection component is used for real-time attack identification and abnormal flow analysis. The abnormal flow cleaning component for the customer reports logs to the service management component. The service management component manages the abnormal flow cleaning service-related configuration, logs the analysis of flow and reports the attack event analysis.

2) Collaboration among the operator and the relevant parties

In the abnormal flow cleaning service, the relevant parties include the customer, the operator and the information technology (IT) device provider.

The collaboration agreement should be pre-established between the operator and the IT device provider. The collaboration agreement should include, but is not limited to:

1. clarification of the roles of each entity during service provision;
2. clarification of the responsibilities of each entity during service provision;
3. implementation support, to clarify the necessary support (e.g., functionality feature, supporting system and security solution) of each entity during the service provision.

3) Security mechanisms

The security mechanisms (details can be seen in clause 10) in secure connecting service should include, but are not limited to:

1. authentication;
2. access control;
3. audit.

7.2.3 Process

There are five steps in the process of an abnormal flow cleaning service, as illustrated in Figure 7-4.

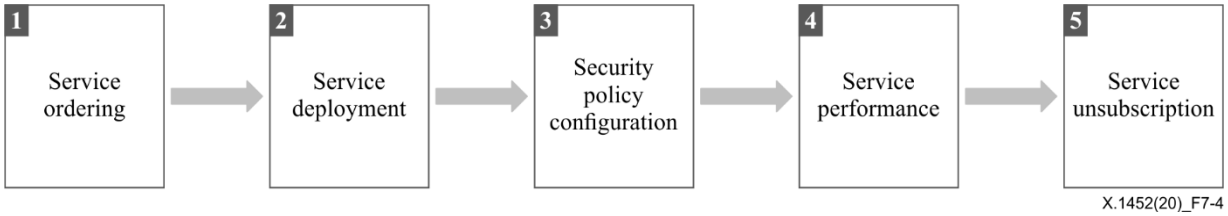

Figure 7-4 – Process of abnormal flow cleaning service

According to Figure 7-4, the process of an abnormal flow cleaning service is as follows:

Step 1: Service ordering

1. The customer orders an abnormal flow cleaning service.

Step 2: Service deployment

1. The service management component assigns an account for the customer ordering an abnormal flow cleaning service.
2. The abnormal flow detecting component copies the customer's flow by mirror or beam split.

Step 3: Security policy configuration

1. The service management component configures the security policy baseline according to the flow distribution, learning through the abnormal flow detecting component.

Step 4: Service performance

1. The customer uses an abnormal flow cleaning service.
2. The customer can check the log analysis of the flow and the report of attack event analysis.

Step 5: Service unsubscription

1. If the customer no longer requires the abnormal flow cleaning service, the customer can unsubscribe from it.

7.3 Security monitoring service

7.3.1 Customer

The customer of a security monitoring service provided by operators is an enterprise customer. This service aims to reduce the security operation risk of the enterprise customer by continuously monitoring security vulnerabilities.

7.3.2 Technical onboarding

1) Pre-deployment

The onboarding of a security monitoring service includes three main scanning components for: port; system vulnerability; and web vulnerability. The security monitoring service can provide functions such as monitoring the operational status and vulnerabilities of the customer's assets and services from the network level and the equipment level, including port scanning, system vulnerability scanning and web vulnerability scanning.

Figure 7-5 illustrates the onboarding of a security monitoring service.

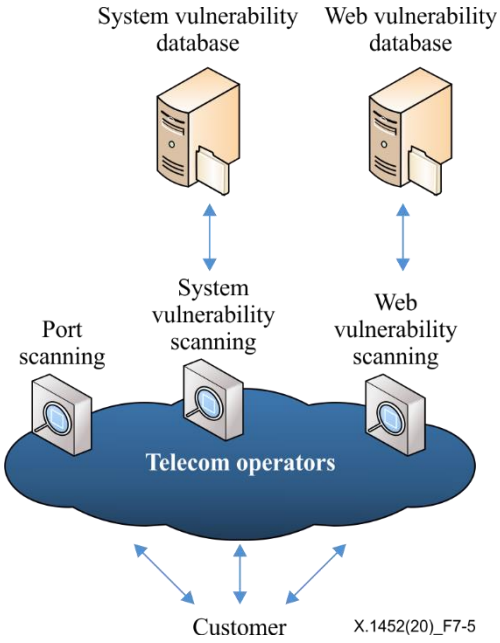

Figure 7-5 – Technical onboarding of security monitoring service

In Figure 7-5, the operator side has scanning components for: the port; system vulnerability; and web vulnerability. These can be implemented by software or hardware devices. The device number and performance to be deployed can be dynamically adjusted, based on parameters such as the number of customers, number of monitored assets and the complexity of the monitored systems.

Each component is described in detail as follows.

– Port scanning component: The main function of the port scanning component is to detect the ports of the monitored assets from the network level and identify the running service information of the open port as much as possible. Port scanning usually needs pre-configuration for common scan policies. The configuration includes the destination Internet protocol (IP) address range, port range, scan options, scan concurrent connections and scan interval. The specific values can be adjusted and configured according to task requirements.

– System vulnerability scanning component: The main function of the system vulnerability scanning component is to scan and analyse the installation and configuration of the operating system, database and application software of the monitored assets from the device level to

discover potential security vulnerabilities. Meanwhile, system vulnerabilities are graded based on the significance of the equipment and the severity of vulnerabilities, etc. The system vulnerability scanning component usually needs to integrate a common system vulnerability database in advance and provide an update and upgrade mechanism for it. Moreover, the system vulnerability scanning component needs to be preconfigured for common scan policies. The configuration content includes the scan target IP address range, port range, scan options, scan vulnerability library selection, scan concurrent connection number and scan task execution time. The specific values can be adjusted and configured according to task requirements.

– Web vulnerability scanning component: The main function of the web vulnerability scanning component is to detect ports and services that are open to monitored assets from the network level. Alongside this function, web vulnerabilities are detected and graded by using the integrated web vulnerability database for attack attempts on the corresponding ports and services without affecting the normal operation of the business. The web vulnerability scanning component usually needs to integrate a common web vulnerability database in advance and provide an update and upgrade mechanism for it. The web vulnerability scanning component also needs to be preconfigured for common scan policies. The configuration content includes web service IP address information, scan options, scan vulnerability library selection, scan concurrent connection number, scan attempts and scan task execution time. The value can be adjusted and configured according to task requirements.

For the enterprise customer side, there is no need to deploy any service device. The enterprise customer only needs to provide the address information of the assets and services to be monitored, including the IP address segment and port range.

2) Collaboration among the operator and the relevant parties

In the security monitoring service, the entities include the port scanning component, the system vulnerability scanning component, the web vulnerability scanning component, the system vulnerability database and the web vulnerability database. Accordingly, the mapping between the entities and the relevant parties is illustrated in Figure 7-5. In Table 2, the symbol "✓" indicates that the entity is related to a particular relevant party.

Table 2 – The mapping between the entities and the relevant parties

Entity	Relevant party	
	Operator	**Third party security service provider**
Port scanning component	✓	
System vulnerability scanning component	✓	
Web vulnerability scanning component	✓	
System vulnerability database		✓
Web vulnerability database		✓

The collaboration agreement should be pre-established between the operator and the third party service provider. The collaboration agreement should include, but is not limited to:

1. clarification of the roles of each entity during service provision;
2. clarification of the responsibilities of each entity during service provision;
3. implementation support, to clarify the necessary support (e.g., functionality feature, supporting system and security solution) of each entity during service provision.

3) Security mechanisms

The security mechanisms (details can be seen in clause 10) in the security monitoring service should include, but are not limited to:

1. authentication;
2. access control;
3. audit.

7.3.3 Process

There are five steps in the process of the security monitoring service, as illustrated in Figure 7-6.

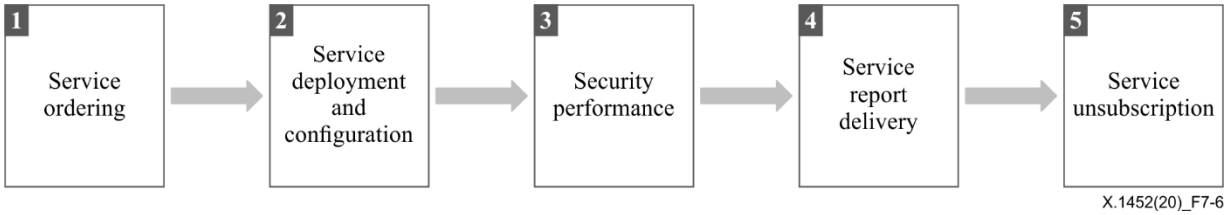

Figure 7-6 – Process of security monitoring service

According to Figure 7-6, the process of a security monitoring service is as follows:

Step 1: Service ordering

1. The customer orders a security monitoring service.

Step 2: Service deployment and configuration

1. The customer provides information of the assets and services to be monitored, such as IP address and assets.

The service provider configures the service policy and delivers the policy to the scanning devices.

Step 3: Service performance

1. The service provider takes customized security scanning of customer's assets according to the service policy.
2. The service provider analyses the security scanning results and forms the security monitoring report.

Step 4: Service report delivery

1. The service provider delivers the monitoring report to the customer.

Step 5: Service unsubscription

1. If the customer no longer requires the security monitoring service, the customer can unsubscribe from it.

7.4 Anti-malicious mobile application service

7.4.1 Customer

The customer of the anti-malicious mobile application service provided by operators is the individual customer. This service aims to protect the individual customer's mobile application from malicious attack through malicious code.

7.4.2 Technical onboarding

1) Pre-deployment

The onboarding of an anti-malicious mobile application service includes four main parts: the user equipment (UE); mobile application platform or store; malicious code scanning component; and the security centre.

The mobile application platform or store offers mobile applications to the individual customer. The malicious code scanning component is used for real-time malicious code detection, and reports such code of the mobile application to the security centre. The malicious code scanning component usually needs to integrate a common malicious code database in advance and provide an update and upgrade mechanism for it. The security centre informs the UE of the malicious mobile application; the UE can then block the installation of the malicious application.

Figure 7-7 illustrates the onboarding of an anti-malicious mobile application service.

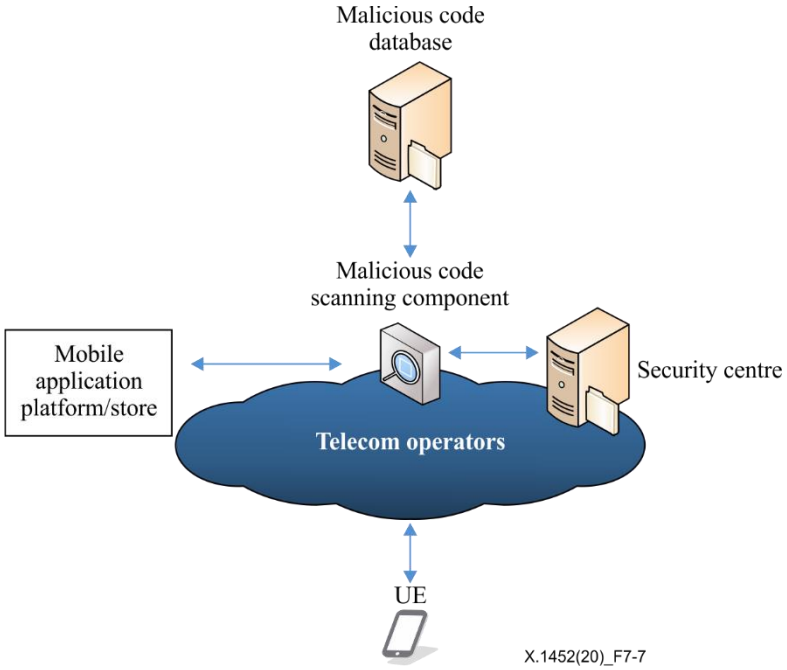

Figure 7-7 – Technical onboarding of anti-malicious mobile application service

2) Collaboration among the operator and the relevant parties

In the anti-malicious mobile application service, the entities include the UE, mobile application platform or store, malicious code scanning component, the security centre and the malicious code database. Accordingly, the mapping between the entities and the relevant parties is illustrated in Figure 7-7. In Table 3, the symbol "✓" indicates that the entity is related to a particular relevant party.

Table 3 – The mapping between the entities and the relevant parties

Entity	Relevant party		
	UE provider	Operator	Third party service provider
UE	✓		
Malicious code scanning component		✓	
Security centre		✓	
Mobile application platform/store			✓
Malicious code database			✓

A collaboration agreement should be pre-established between the operator and the UE provider, and also between the operator and the third service party provider. The collaboration agreement should include, but is not limited to:

1. clarification of the roles of each entity during service provision;
2. clarification of the responsibilities of each entity during service provision;
3. implementation support, to clarify the necessary support (e.g., functionality feature, supporting system and security solution) of each entity during service provision.

3) Security mechanisms

The security mechanisms (details can be seen in clause 10) in the anti-malicious mobile application service should include, but are not limited to:

1. authentication;
2. access control;
3. audit.

7.4.3 Process

There are five steps in the process of the anti-malicious mobile application service, as illustrated in Figure 7-8.

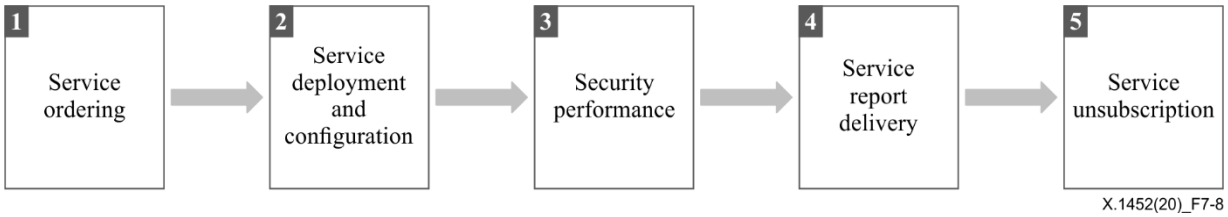

Figure 7-8 – Process of anti-malicious mobile application service

According to Figure 7-8, the process of anti-malicious mobile application service is as follows:

Step 1: Service ordering

1. The customer orders anti-malicious mobile application service.

Step 2: Service deployment and configuration

1. The malicious code scanning component configures the service policy (e.g., the algorithm of malicious code scan, the format of the malicious code detection report) and delivers the policy to the security centre.

Step 3: Service performance

1. The malicious code scanning component undertakes malicious code scanning of the customer's mobile application according to the service policy.
2. The malicious code scanning component analyses the scanning results and delivers the scanning report to the security centre.

Step 4: Service report delivery

1. The security centre informs the UE of the malicious mobile application; the UE can then block the installation of the malicious application.

Step 5: Service unsubscription

1. If the customer no longer requires the anti-malicious mobile application service, the customer can unsubscribe from it.

8 Reference model of security service

A reference model of a security service offered by an operator is shown in Figure 8-1.

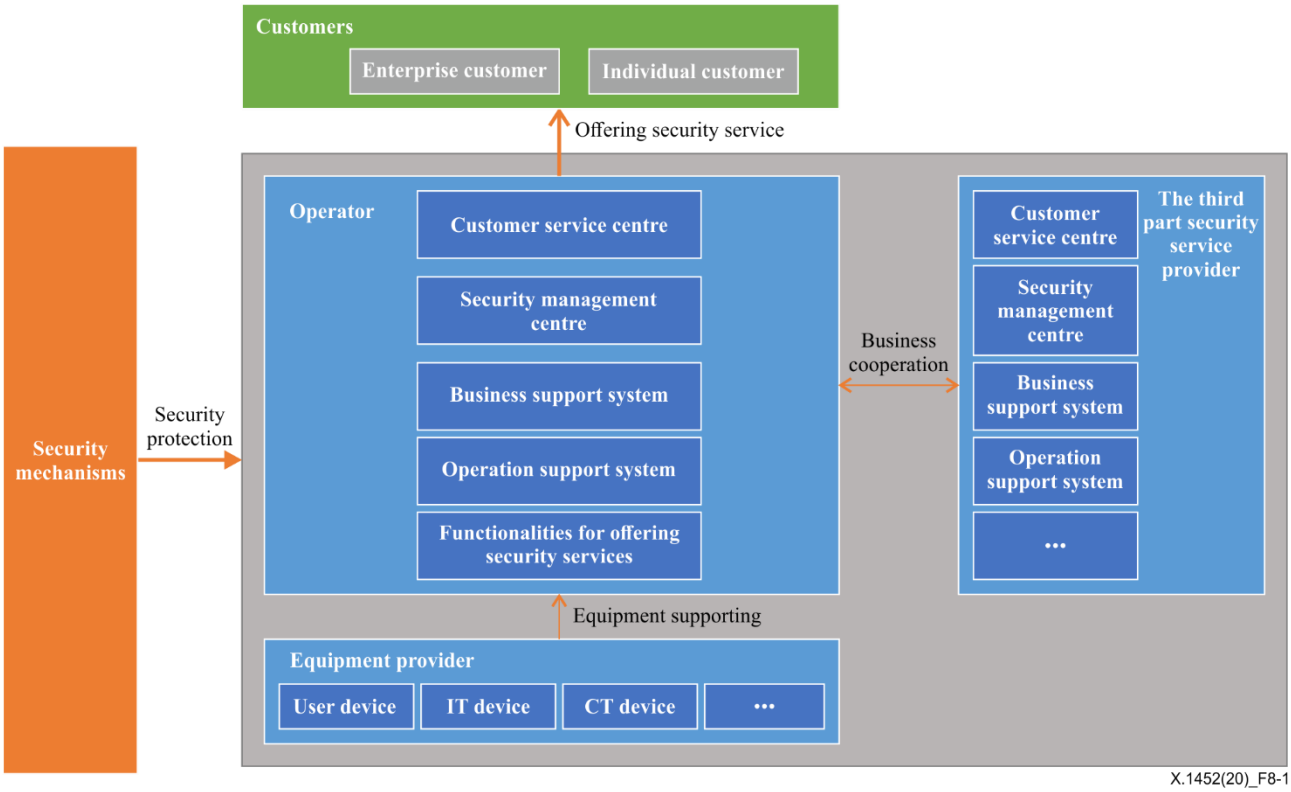

Figure 8-1 – Reference model of security service

In this model, three modules are involved:

– the customer;

– the stakeholders in service provision; and

– the security mechanism.

The potential customer type may include the individual customer and the enterprise customer.

Stakeholders in service provision include the operator, the equipment provider and the third party security service provider. The equipment provider may act as a UE provider, IT device provider, communication technology (CT) device provider and the operator. The third part security service provider is optional according to the security service requirements.

1) The operator is the core part of the service components; it contains the following sub-components:
   1. functionalities for offering security services;
   2. operation support system;
   3. business support system;
   4. security management centre;
   5. customer service centre.

2) The equipment provider offers necessary devices to support the security services, it contains following sub-components:
   1. the user device, such as mobile phone, SIM or USIM card;
   2. IT device;

3. telecommunication device;
4. others.

3) The third party security service provider cooperates with the operator to support the security services; it contains following sub-components:

1. operation support system;
2. business support system;
3. security management centre;
4. customer service centre;
5. others.

The security mechanisms contain the technical schemes to mitigate potential threats to the security service offered by the operator.

9 Requirements for stakeholders

9.1 The operator

9.1.1 Functionalities to offer security services

(1) Governance, risk and compliance functionalities

It is required that the operator has the functionalities of whole lifetime security governance, risk management and security compliance management for its security services.

(2) Analysis and testing functionalities

It is required that the operator has the functionalities to:

– analyse the user, requirements, deployment scheme, process, etc. for a given security service; and

– test the functionality and procedures of the usage of a given security service.

(3) Data functionalities

It is required that the operator has the functionalities of data collection, analysis, storage, etc. to support secure service functionality.

(4) Network functionalities

It is required that the operator has network functionalities to support the secure service functionality that include, but are not limited to:

– abnormal flow analysis, cleaning;

– network access.

(5) End-point or mobile functionalities

It is required that the operator has end-point or mobile functionalities to support the secure service functionality including, but not limited to:

– port scanning;

– system vulnerability scanning.

(6) Identity functionalities

It is required that the operator has identity functionalities to support the secure service functionality that include, but are not limited to:

– identity authentication;

– identity management.

9.1.2 Operation support system

The operation support system offers the necessary functions for the telecommunication services of operator, and needs to offer the interface and function to support the security services.

9.1.3 Business support system

The operator may deploy the business support system alone or jointly with the operation support system. The business support system needs to offer the interface and function to support security services.

9.1.4 Security management centre

The security management centre offers security management functions of the operator's business, and manages the security mechanisms of the security service.

9.1.5 Customer service centre

The customer service centre supports the customer's requirements. The security service provided by the operator can be newly deployed or shared with the customer service centre.

9.2 The equipment provider

9.2.1 User equipment

UE offers the mobile phone, and a SIM or USIM card.

9.2.2 Information technology device

The IT device offers a server, display device, chip, software system, etc. to support the security service.

9.2.3 Telecommunication device

The telecommunication device offers telecommunication-related devices such as a base station or core network device.

9.3 The third part security service provider

9.3.1 Operation support system

The operation support system offers functions necessary for the security services of the third party security service provider, and needs to offer the interface and function to support the security services.

9.3.2 Business support system

The business support system of the third part security service provider needs to offer an interface and function to support the security services.

9.3.3 Security management centre

The security management centre of the third part security service provider manages the security mechanisms of the security service.

9.3.4 Customer service centre

The customer service centre supports customer requirements.

10 Security mechanisms

The security mechanisms provide security protection for services offered by operators. The security mechanisms can be provided as the basic building blocks for stakeholder selection.

10.1 Authentication

Authentication provides assurance of the claimed identity of an entity. Some security technologies that may be applied include:

– the use of authentication information, such as passwords supplied by a sending user and checked by the receiving user;

– cryptographic technologies; and

– the use of characteristics or possessions of the user and single sign on.

For more details of the authentication framework, see [b-ITU-T X.811].

10.2 Access control

Access control provides access rights of the entity to prevent the unauthorized use of a resource. If the entity attempts to use an unauthorized resource or an authorized resource with an improper type of access, the access control function will then reject the attempt and may additionally report the incident for the purposes of generating an alarm or recording it as part of a security audit trail.

For more details of the access control framework, see [b-ITU-T X.812].

10.3 Security audit trails

Security audit trails provide a security mechanism to permit detection and investigation of breaches of security by permitting a subsequent security audit.

A security audit is an independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to aid in damage assessment, and to recommend any indicated changes in controls, policy and procedures.

For more details of the security audit trails framework, see [b-ITU-T X.816].

10.4 Authorization

The authorization function may use the authenticated identity of or information about users (such as membership within a known set of users) or user capabilities, in order to determine and enforce their access rights. If a user attempts to use an unauthorized resource or an authorized resource with an improper type of access, the access control function will then reject the attempt and may additionally report the incident for the purposes of generating an alarm or recording it as part of a security audit trail.

The access control function may be based on the use of the following items:

a) access control information bases, where the access rights of peer entities are maintained in a database;

b) authentication information, such as passwords, the possession and subsequent presentation of which is evidence of the accessing user's authorization;

c) capabilities, the possession and subsequent presentation of which is evidence of the right to access the user or resource defined by the capability;

d) security labels, which, when associated with a user, may be used to grant or deny access, usually according to a security policy;

e) time of attempted access;

f) route of attempted access;

g) duration of access; and

h) physical location of attempted access.

For more details of the authorization mechanism, see [b-ITU-T X.800].

10.5 Availability

Ensure that the ability to manage the network device or communications link of security service by authorized personnel or devices cannot be denied.

Techniques used to access control may contribute to providing availability.

For more details of availability framework, see [b-ITU-T X.800].

10.6 Blacklist mechanism

Provides an identification of a list of persons or sources in services, where the identifications of the list are denied access to particular resources.

10.7 Communication security

Protect the communication link and the communication data of the security service from unauthorized access or viewing.

Techniques used to address encryption may contribute to providing communication confidentiality.

10.8 Data confidentiality

Protect the network device or communications link configuration information from unauthorized access or viewing.

Protect the administrative authentication information (e.g., administrator identifications and passwords) from unauthorized access or viewing.

Techniques used to address access control may contribute to providing data confidentiality.

For more details of the confidentiality framework, see [b-ITU-T X.814].

10.9 Data integrity

Protect the configuration information of network devices and communications links against unauthorized modification, deletion, creation and replication.

The same type of consideration is applied to administrative authentication information (e.g., administrator identifications and passwords).

Techniques used to address access control may contribute to providing data confidentiality.

For more details of the integrity framework, see [b-ITU-T X.815].

10.10 Non-repudiation

Provide a record identifying the activity of the subscription, the usage of the security service and the action that was performed. This record can be used as proof of the originator of the administrative or management activity.

The non-repudiation may use the digital signature method or the certification method.

For more details of the non-reputation framework, see [b-ITU-T X.813].

10.11 Privacy protection

Ensure that information that can be used to identify the user is not available to unauthorized personnel or devices.

Techniques used to address encryption, access control and user consent may contribute to providing privacy protection.

10.12 Relationship of security mechanisms to the stakeholders

The relationship of security mechanisms and stakeholders of security service are shown in Table 4.

In Table 4, the letter "Y" (Yes) indicates that the security mechanism is related to a particular stakeholder.

Table 4 – Relationship of security mechanisms to entities

Security mechanisms	Stakeholder		
	Operator	**Equipment provider**	**Third party service provider**
Authentication	Y		Y
Access control	Y		Y
Security audit trails	Y		Y
Authorization	Y	Y	Y
Availability	Y	Y	Y
Blacklist mechanism	Y		Y
Communication security	Y		Y
Data confidentiality	Y	Y	Y
Data integrity	Y	Y	Y
Non-repudiation	Y		Y
Privacy protection	Y	Y	Y

11 Reference procedures

For operators to offer security services, an adaptive mechanism is introduced to accommodate the constantly emerging new technologies and collaboration among relevant entities. It consists of seven procedures as shown in Figure 11-1.

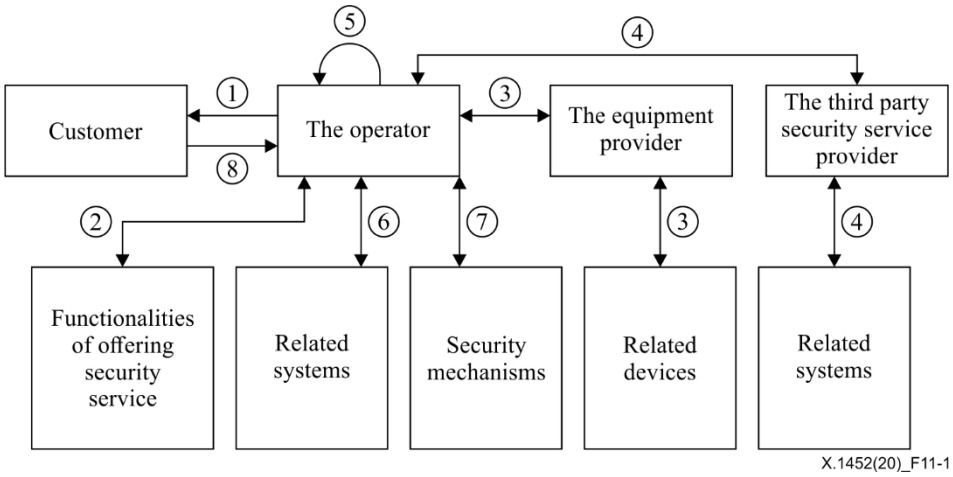

Figure 11-1 – Reference procedures of security services provided by operators

Procedure 1: Identify customer

The operator identifies the customer's requirement, and classifies the potential customer type, which may include the individual customer and the enterprise customer of security functionality usage.

Procedure 2: Identify secure functionality

The operator identifies its functionalities, such as data functionality, network functionality and end-point functionality, that can act as the basic functionalities for the security service.

Procedure 3: Onboarding with the equipment provider

The operator identifies and implements the pre-deployment or pre-configuration necessary for certain security services with the equipment provider, the collaboration agreement between operator and the equipment provider and the necessary security mechanisms for a certain security service.

Procedure 4: Onboarding with the third part security service provider

The operator identifies and implements the pre-deployment or pre-configuration necessary for certain security services with the third part security service provider, the collaboration agreement between operator and the third part security service provider and the necessary security mechanisms for a certain security service.

Procedure 5: Service functions design and development

Design the functions of the security services according to the security functionality.

Based on the functions of the security services, develop or prepare (collaborate with the equipment provider) the specific security device or the component for the security service, and identify the security mechanisms to support the service.

Design the security service processes including service ordering, service deployment and configuration, service performance, service report delivery and service unsubscription.

Procedure 6: Connect with related supporting system

Design and test the interface between the security service and operator's related support system, e.g., operation support system, business support system, customer service centre, and connect the security service with the related support system.

Procedure 7: Security mechanisms deployment

The security mechanisms could be the basic building blocks for stakeholder selection, based on the functions of the security services; relevant stakeholders deploy security mechanisms. The relationship of the security mechanisms can be seen in Table 4, since the security service provided by the operators may have been customized and may have continuously evolved, the security mechanisms need case-by-case analysis and selection.

Procedure 8: Deliver the security service to the customer.

The operator delivers and offers the security service to the customer.

Bibliography

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.811] Recommendation ITU-T X.811 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*.

[b-ITU-T X.812] Recommendation ITU-T X.812 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework*.

[b-ITU-T X.813] Recommendation ITU-T X.813 (1996), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework*.

[b-ITU-T X.814] Recommendation ITU-T X.814 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Confidentiality framework*.

[b-ITU-T X.815] Recommendation ITU-T X.815 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Integrity framework*.

[b-ITU-T X.816] Recommendation ITU-T X.816 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Security audit and alarms 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, 2021