International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1332

(03/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Smart grid security

Security guidelines for smart metering services in smart grids

Recommendation ITU-T X.1332

International Telecommunication Union

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.1332

Security guidelines for smart metering services in smart grids

Summary

Smart metering services have been widely deployed worldwide to make electricity grids more efficient and reliable by gathering/providing electricity usage information from/to customers, respectively. This information can be used to estimate customers' electricity demands, and the estimation can be used to shift demand or to change customers' electricity consumption behaviour by providing electricity usage information to them. However, smart metering services can malfunction because of various threats. For example, invalid metering information can lead to erroneous demand management decisions, and abusing load control functions can cause economic and physical damage to customers. Recommendation ITU-T X.1332 provides security guidelines for smart metering services to enable service providers to implement appropriate security measures to ensure the security of their service. This Recommendation identifies security threats and attack methods against smart metering services, and specifies security requirements and capabilities to mitigate these threats and attacks accordingly.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1332	2020-03-26	17	11.1002/1000/14086

Keywords

Advanced metering infrastructure, security guidelines, smart grid, smart metering service.

* 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.1332

Security guidelines for smart metering services in smart grids

1 Scope

This Recommendation provides security guidelines for smart metering services in smart grids. It covers the following:

– identification of security threats and attacks against smart metering services;

– security requirements for smart metering services; and

– security guidelines for smart metering services to meet security requirements.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 demand response (DR) [b-ITU-T Y.2071]: A smart grid feature that allows consumers to reduce or change their electrical use patterns during peak demand, usually in exchange for a financial incentive. Mechanisms and incentives for utilities, business, industrial, and residential customers to cut energy use during times of peak demand or when power reliability is at risk. Demand response is necessary for optimizing the balance of power supply and demand.

3.1.2 electric power system operator [b-IEC 60050-617]: A party responsible for safe and reliable operation of a part of the electric power system in a certain area and for connection to other parts of the electric power system.

3.1.3 energy management system (EMS) [b-ITU-T Y.2071]: A computer system comprising a software platform providing basic support services and a set of applications providing the functionality needed for the effective operation of electrical generation and transmission facilities so as to assure adequate security of energy supply at minimum cost.

3.1.4 smart meter [b-ITU-T X.1331]: A device installed in premises to monitor and control the electrical power usage of smart home devices based on their demand response information.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 data concentrator: An intermediate device located between a smart meter and the utility systems whose main purpose is to collect and manage the data received from the smart meter.

3.2.2 meter data management system (MDMS): A meter data management system (MDMS) aggregates, validates, estimates and permits editing of meter data such as energy usage, generation, and meter logs. An MDMS stores this data for a limited amount of time before it goes to a data warehouse and makes this data available to authorized systems.

NOTE – Adapted from [b-ITU-T Y.2071]

3.2.3 smart metering service: A service which gathers electricity usage data through smart meters and provides analysed information to customers and utilities; third-party service providers

may also participate in this service to use the electricity usage data for the provision of a service or a set of services to the customer.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CDMA Code-Division Multiple Access

DDoS Distributed Denial of Service

DoS Denial of Service

EMS Energy Management System

EUIS Energy Usage Information System

HMAC Hash-based Message Authentication Code

IHD In-Home Display

LTE Long-Term Evolution

MDMS Meter Data Management System

PII Personally Identifiable Information

PLC Power Line Communication

QoS Quality of Service

TLS Transport Layer Security

VPN Virtual Private Network

5 Conventions

None.

6 Overview

Smart metering services, one of the fundamental features in a smart grid, have been widely deployed worldwide to make electricity grids more efficient and reliable by gathering/providing information from/to customers, respectively.

A smart meter measures, records, and transfers the amount of electricity that a customer has used. Metering data is transmitted periodically, such as every 5 or 15 minutes. Based on these data, smart metering service providers can estimate customers' electricity demands. According to this estimation, they can make the electricity grid more reliable by shifting the demand or by changing customers' electricity consumption behaviour.

Smart metering service providers can provide customers with information about their electricity usage as well as real-time electricity rates, estimated bills, statistical data, or demand trends. By using this information, customers can voluntarily try to reduce their electricity consumption. For example, if the provider applies dynamic pricing and changes the rate based on the electricity demands, customers might delay or advance their electricity-consuming action.

However, threats exist that could cause smart grids to malfunction. For example, invalid metering information can lead to erroneous demand management decisions, and abusing load control functions can cause economic and physical damage to customers. Further, when third-party service providers have access to metering information, the issue of protecting personally identifiable information (PII) must be considered.

Moreover, electricity usage information, statistics, and cost information are usually transferred to customers' Internet-connected devices such as smartphones or handheld PCs. Thus, almost all threats that can affect mobile devices could also affect smart metering services.

This Recommendation investigates security threats in smart metering services and identifies security requirements and capabilities to ensure the security of smart metering services.

7 Architecture of smart metering services

Before describing the security of smart metering services, an architecture for such services is defined to identify all entities related to smart metering service to clarify their relationships.

For defining a general model of a metering service, this Recommendation considers the following use cases:

– gathering electricity usage data from metering devices;

– providing electricity usage trends to customers;

– providing electricity usage information to third-party service providers; and

– providing electricity usage information to electric power system operators.

Figure 7-1 shows a smart metering service architecture for these use cases. In this model, there are six major entities: metering device, electric power system operator, metering data management system (MDMS), utility (system), third-party service provider and customer.

Metering device measures a customer's electricity usage and sends metering data to MDMS in a utility. The utility provides an energy usage information system (EUIS) to present electricity usage trends to customers. To generate statistical information, EUIS obtains metering data from MDMS. The utility's billing system also uses metering data. In this architecture, the EUIS and the billing system are categorized as utility system.

Electric power system operator uses metering data to estimate the current and future status of the power system. Electric power system operator's energy management system (EMS) receives metering data from MDMS and analyses electricity demand trends using these data. Based on the estimated demands, the operator adjusts the amount of electricity supply so that the power system can balance supply and demand.

Customer has smart energy displays or smart devices that show statistics of energy usage and control the loads connected to their premises networks. Customers can use several types of displays, including smartphones, tablets, smart TVs, personal computers, and specialized in-home displays (IHDs) to access the utility's EUIS.

Third-party service provider uses metering data to improve service quality. For example, a cable TV company can broadcast a commercial advertisement for a detergent to a particular customer, if it knows this customer is doing his laundry.

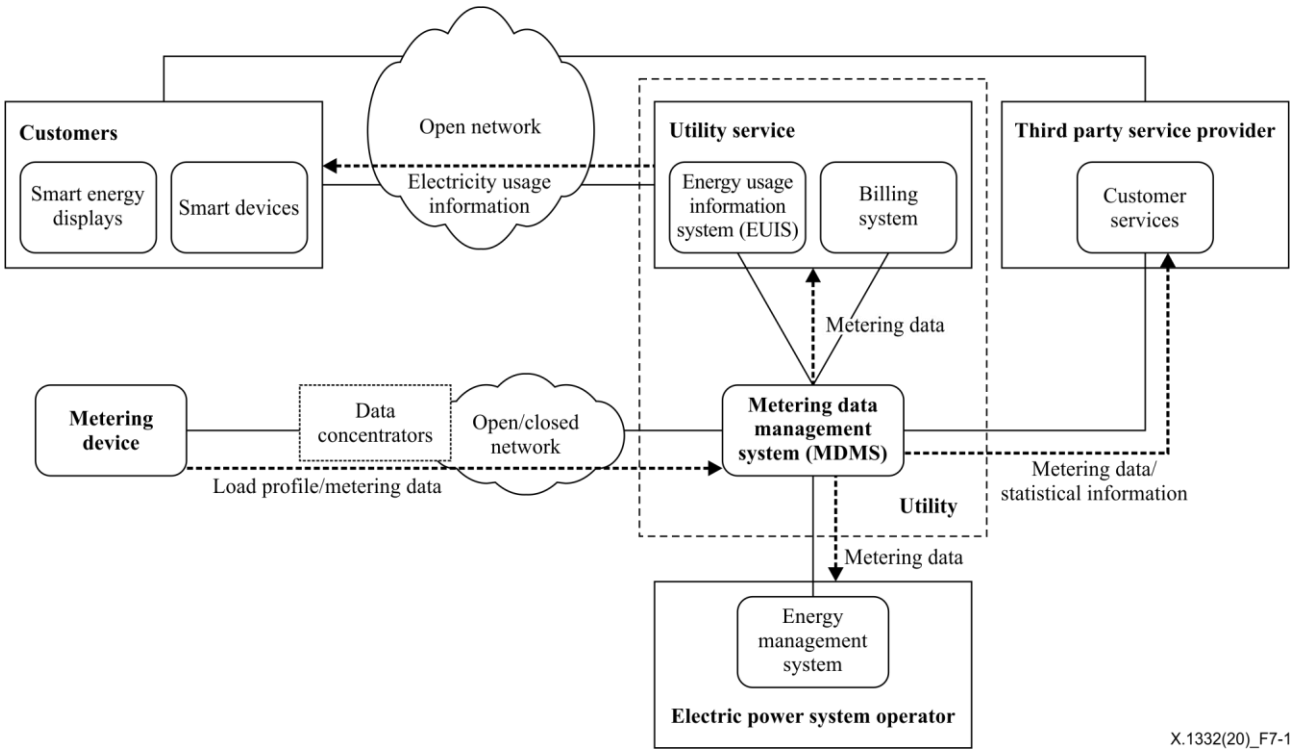

Figure 7-1 – Smart metering service architecture

Six relationships between entities in this architectural model are considered: metering device and MDMS, MDMS and EMS, MDMS and utility system, MDMS and third-party service provider, customer and utility system, and customer and third-party service provider.

Metering device is connected to MDMS via a network. The network can be an open one such as LTE or CDMA or a closed one such as PLC or leased line. Irrespective of the network type, data concentrators will aggregate metering data in an area and send the aggregated data to MDMS.

MDMS and EMS communicate with each other via a telecommunication network with guaranteed quality of service (QoS).

MDMS and utility system are usually located in the same network. If they are not connected in the same network, they are usually connected with a telecommunication network with guaranteed QoS.

MDMS can be connected with third-party service providers using a telecommunication network with guaranteed QoS.

Since customers use an open network such as the Internet, both utility system and third-party service provider are connected with customers via the open network. Customers can access the networks via WiFi, LTE, Bluetooth, etc.

8 Security threats in smart metering services

8.1 Threats to interface between metering device and MDMS

The interface between the metering device and MDMS is used to collect and process a large number of customers' electricity usage data, including meter data, load profile, and electricity quality measurements. The data transferred via this interface is the attackers' main target. Attackers damage smart metering services by intercepting, falsifying and replaying these data.

Attackers also target denial of smart metering services by launching distributed denial of service (DDoS) attacks against MDMS.

The interface between metering device and MDMS is vulnerable to the following threats:

– Information leakage: Smart metering devices (i.e., smart meter) periodically send electricity load data (metering data) to MDMS via a data concentrator. In smart grids, this period is very short (e.g., 5 min or less). Therefore, attackers can notice customers' life pattern if they can sniff metering data.

– Falsifying metering data: Attackers can block actual metering data, and send falsified metering data to MDMS instead. Such attacks can cause failure of demand estimation by preventing MDMS and EMS from accessing the actual collected metering data. Such failures can also cause an imbalance between demand and supply, resulting in power outage.

– Falsifying load profile: Attackers can make unauthorized modifications to the load profile stored in metering devices. Since billing system charges each customer based on their load profile, this threat could result in incorrect billing of customers.

– Denial of service (DoS): Attackers can perform a DoS attack to run malicious code on a number of metering devices or data concentrators and flood a target (usually the MDMS) with considerable data or a large number of service requests. Such an attack can slow down or even stop a smart metering service.

8.2 Threats to interface between MDMS and third-party service provider

The interface between MDMS and third-party service provider is used to share metering data so that the latter can provide various customized services for each customer. Since PII can be transferred via this interface, attackers mainly target these data and damage smart metering services by intercepting and using these data.

The interface between MDMS and third-party service provider is vulnerable to the following threats:

– PII breaches: Attackers can intercept PII by launching a packet sniffing attack or executing a malicious code on third-party service provider's Internet-connected systems.

8.3 Threats to interface between utility system and customer

The interface between the utility system and customer premises device provides various types of information that encourage customers to participate in demand response. Information including customer's electricity usage trends, real-time electricity prices, demand trends, bills and statistical data can be provided. By falsifying transferred information, attackers can deceive a customer into consuming excessive electricity. DoS attack is another serious potential threat to utility system connected to customer premises devices.

The interfaces between utility system and customer device is vulnerable to the following threats:

– Falsifying real-time price: Attackers can falsify real-time price communicated by the utility system to customers to deceive them. If falsified price is made lower than actual price, customer devices (such as a smart energy display) can make an electricity-consuming device (e.g., electric vehicle) consume more electricity. By contrast, if the price is made higher than actual price, customer could lose the chance to store electricity at low cost.

– Denial of service: Attackers can perform a DoS attack to run malicious code on a number of customer devices and flood a target (usually an EUIS) with massive service requests. Such attack can slow down or even stop a smart metering service.

– PII breaches: An attacker can intercept PII by launching a packet sniffing attack or executing malicious code on a customer's Internet-connected device.

9 Security requirements of smart metering services

9.1 Security requirements of electricity usage metering

Electricity usage metering is the most important feature of smart metering services. When it works properly, MDMS can collect the necessary information for producing electricity usage trends, each customer's usage pattern, electricity utility bills, etc. Furthermore, other entities in the smart metering service can use this information to play their role correctly. Thus, the integrity, authenticity, and confidentiality of metering data are the main security requirements of the information gathering procedure.

To correctly respond to threats against the communication interface between smart meter and MDMS, the following security requirements should be considered.

– End-to-end confidentiality of data transferred via communication interface between a smart meter and the MDMS should be ensured.

– End-to-end integrity of communication messages between a smart meter and the MDMS should be ensured to prevent unauthorized modification of the data.

– Metering data and authentication information stored in devices such as smart meters, data concentrators, and MDMS should be protected from unauthorized access.

– Sender's authenticity for each communication transaction should be ensured.

9.2 Security requirements for information used by customer

Since customer devices can access a utility system connected to the backend electric power system, they are the main target for attacking smart metering services. Thus, for this part of a smart metering service, data and applications in customer devices should be protected.

To mitigate possible side effects from threats against the communication interface between the utility system and customer, the following security requirements should be considered.

– Data confidentiality for the communication interface between the customer and utility system should be ensured.

– Data integrity for communication messages between the customer and utility system should be ensured to prohibit unauthorized modification of data.

– Sender's authenticity for each communication transaction should be ensured.

– Information stored in a customer device and utility system should be protected from unauthorized access.

– Integrity of applications in customer device should be considered.

9.3 Security requirements for information used by third-party service provider

The main concerns in this matter are PII data handling and PII breaches between third-party service provider and MDMS.

To properly handle threats against the communication interface between MDMS and third-party service provider, the following security requirements should be considered.

– Data confidentiality for the communication interface between MDMS and third-party service provider should be ensured.

– Data integrity for communication messages between the MDMS and third-party service provider should be ensured to prohibit unauthorized modification of data.

– Sender's authenticity for each communication transaction should be ensured.

– For realizing personalized services, PII data should be handled properly for only disclosed purpose with customer's consent.

– For services that do not use PII, metering-related PII should not be provided.

9.4 Security requirements for information used by electric power system operator

To properly prevent threats against the communication interfaces between MDMS and electric power system operator, the following security requirements should be considered.

– Data confidentiality for the communication interface between MDMS and electric power system operator should be ensured.

– Data integrity for the communication messages between MDMS and electric power system operator should be ensured to prohibit unauthorized modification of data.

– Only authorized entities should be allowed to access communication interface between MDMS and electric power system operator.

– Metering-related PII should not be provided.

10 Security guidelines for smart metering services

10.1 Security controls for electricity usage metering

To fulfil the security requirements of electricity usage metering, the following security controls should be considered as capabilities of each entity for electricity metering.

– Access control for metering data should be applied to metering devices, data concentrators, and MDMS. Only authorized entities should be allowed access to electricity usage data.

– Mutual authentication mechanism between metering device and MDMS should be used to ensure sender's authenticity.

– Message authentication measures should be taken to protect integrity of electricity usage data transferred to MDMS. For example, cryptographic message authentication codes such as HMAC may be an option for this regard.

– Data encryption may be considered as a security measure to protect billing-related data.

– Detection of damage to data integrity and decryption of encrypted data should be performed at MDMS.

– Secure key management mechanism should be adopted in metering devices, data concentrators and MDMS for securely generating, agreeing upon, storing and refreshing of cryptographic keys.

– Data protection mechanism should be used to ensure confidentiality and integrity of metering data stored in MDMS.

– Security measure to mitigate DoS attack may be adopted at MDMS.

10.2 Security controls for information used by customer

To fulfil security requirements for information used by the customer, the following security controls should be considered as capabilities of each entity:

– Secure communication measures such as TLS should be applied to communication between customer device and utility system. Mutual authentication, communication data authentication and encryption should be provided between customer device and utility system.

– User authentication and authorization for accessing electricity usage information should be applied to applications that provide this information. Utility system should authorize users to access only their own data.

– User authentication data and cryptographic keys for user authentication and secure communication as well as PII should be securely stored in customer's device.

– Integrity check measures should be initiated to detect falsification of an application whenever it is run on the customer's device.

10.3 Security controls for information used by third-party service provider

To fulfil security requirements for information used by a third-party service provider, the following security controls should be considered as capabilities of each entity:

– A leased line may be used to prevent unauthorized users from accessing the connection between MDMS and third-party service provider.

– Secure communication measures such as a virtual private network (VPN) should be applied to the communication between customer device and utility system. Mutual authentication, communication data authentication and encryption should be provided between customer device and utility system.

– PII protection process should be applied throughout its entire lifecycle if PII is accessed by third-party service provider [b-GAO-08-343]. De-identification may be applicable if identification data is not needed by third-party service provider.

10.4 Security controls for information used by electric power system operator

To fulfil security requirements for information used by electric power system operator, the following security controls should be considered as capabilities of each entity:

– A leased line should be used to reduce the risk of unauthorized access to the connection between MDMS and electric power system operator.

– Secure communication measures such as a VPN should be applied to the communication between MDMS and electric power system operator. Mutual authentication, communication data authentication and encryption should be provided between MDMS and electric power system operator.

– De-identification may be applicable if the identification data is not needed by electric power system operator.

Bibliography

[b-ITU-T X.1331] Recommendation ITU-T X.1331 (2018), *Security guidelines for home area network (HAN) devices in smart grid systems*.

[b-ITU-T Y.2071] Recommendation ITU-T Y.2071 (2015), *Framework of a micro energy grid*.

[b-GAO-08-343] United States Government Accountability Office, GAO-08-343:2008, *Information Security: Protecting Personally Identifiable Information.* https://www.gao.gov/new.items/d08343.pdf

[b-IEC 60050-617] IEC 60050-617:2009, *International Electrotechnical Vocabulary – Part 617: Organization/Market of electricity*.

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