International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.235.10

(03/2022)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Systems aspects

H.323 security: Support of datagram transport layer security (DTLS) for media streams

Recommendation ITU-T H.235.10

ITU-T H-SERIES RECOMMENDATIONS

AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	**H.230–H.239**
Communication procedures	H.240–H.259
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
Systems and terminal equipment for audiovisual services	H.300–H.349
Directory services architecture for audiovisual and multimedia services	H.350–H.359
Quality of service architecture for audiovisual and multimedia services	H.360–H.369
Telepresence, immersive environments, virtual and extended reality	H.420–H.439
Supplementary services for multimedia	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	H.510–H.519
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
VEHICULAR GATEWAYS AND INTELLIGENT TRANSPORTATION SYSTEMS (ITS)	
Architecture for vehicular gateways	H.550–H.559
Vehicular gateway interfaces	H.560–H.569
BROADBAND, TRIPLE-PLAY AND ADVANCED MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619
Advanced multimedia services and applications	H.620–H.629
Content delivery and ubiquitous sensor network applications	H.640–H.649
IPTV MULTIMEDIA SERVICES AND APPLICATIONS FOR IPTV	
General aspects	H.700–H.719
IPTV terminal devices	H.720–H.729
IPTV middleware	H.730–H.739
IPTV application event handling	H.740–H.749
IPTV metadata	H.750–H.759
IPTV multimedia application frameworks	H.760–H.769
IPTV service discovery up to consumption	H.770–H.779
Digital Signage	H.780–H.789
E-HEALTH MULTIMEDIA SYSTEMS, SERVICES AND APPLICATIONS	
Personal health systems	H.810–H.819
Interoperability compliance testing of personal health systems (HRN, PAN, LAN, TAN and WAN)	H.820–H.859
Multimedia e-health data exchange services	H.860–H.869
Safe listening	H.870–H.879

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

Recommendation ITU-T H.235.10

H.323 security: Support of datagram transport layer security (DTLS) for media streams

Summary

Recommendation ITU-T H.235.10 describes the security procedures for the establishment of media streams utilising datagram transport layer security (DTLS).

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T H.235.10	2022-03-16	16	11.1002/1000/14968

Keywords

H.235, H.235.10, H.323, DTLS, security.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T H.235.10

H.323 security: Support of datagram transport layer security (DTLS) for media streams

1 Scope

The scope of this Recommendation is to provide procedures for the establishment of datagram transport layer security (DTLS) [IETF RFC 6347] connections for media streams. DTLS is an evolution of the widely implemented transport layer security (TLS) security protocol that allows the use of a security protocol over a datagram environment.

An important aspect of the establishment of a DTLS connection is that a fingerprint and hash is communicated via an out-of-band means and that the certificate exchange occurs within the established DTLS connection. The fingerprint is used to ensure the integrity of the certificates. DTLS also follows the TLS client-server model for establishment of the DTLS connection where one of the endpoints is responsible for the establishment of the connection. The roles (client or server) need to be negotiated between the endpoints.

In order for endpoints to communicate the fingerprint/hash and roles information, the information needs to be signalled to the peer endpoint. This Recommendation utilises [ITU-T H.245] to signal this information.

This Recommendation also provides DTLS support for the transmission of secure real-time transport protocol (SRTP) keys in order to establish media protected via SRTP. The indication of support for DTLS based SRTP key negotiation is signalled via [ITU-T H.245]. Once the DTLS connection is established endpoints use the procedures defined in [IETF RFC 5764] for SRTP key negotiation during handshake. This Recommendation provides an alternate method to [ITU-T H.235.7] and [ITU-T H.235.8] for SRTP keying.

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 H.235.7] Recommendation ITU-T H.235.7 (2005), *H.323 security: Usage of the MIKEY key management protocol for the Secure Real Time Transport Protocol (SRTP) within H.235*.

[ITU-T H.235.8] Recommendation ITU-T H.235.8 (2005), *H.323 security: Key exchange for SRTP using secure signalling channels*.

[ITU-T H.245] Recommendation ITU-T H.245 (2022), *Control protocol for multimedia communication*.

[ITU-T H.323] Recommendation ITU-T H.323 (2022), *Packet-based multimedia communications systems*.

[IETF RFC 4145] IETF RFC 4145 (2005), *TCP-Based Media Transport in the Session Description Protocol (SDP)*.

[IETF RFC 4301] IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol*.

[IETF RFC 4572] IETF RFC 4572 (2006), *Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)*.

[IETF RFC 5246] IETF RFC 5246 (2005), *The Transport Layer Security (TLS) Protocol Version 1.2*.

[IETF RFC 5764] IETF RFC 5764 (2010), *Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)*.

[IETF RFC 6083] IETF RFC 6083 (2011), *Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)*.

[IETF RFC 6347] IETF RFC 6347 (2012), *Datagram Transport Layer Security Version 1.2*.

[IETF RFC 8261] IETF RFC 8261 (2017), *Datagram Transport Layer Security (DTLS) Encapsulation of SCTP Packets*.

3 Definitions

3.1 Terms defined elsewhere

All DTLS-related terms used in this Recommendation are based on [b-IETF tls-terms].

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ABNF Augmented Backus-Naur Form

DTLS Datagram Transport Layer Security

IPsec Internet Protocol Security

OLC H.245 OpenLogicalChannel message

OLCAck H.245 OpenLogicalChannelAck message

SCTP Stream Control Transmission Protocol

SDP Session Description Protocol

SIP Session Initiation Protocol

SRTCP Secure Real-time Transport Control Protocol

SRTP Secure Real-time Transport Protocol

TCS Terminal Capability Set

TLS Transport Layer Security

UDP User Datagram Protocol

5 Conventions

None.

6 Overview

This Recommendation defines procedures based on those defined by [IETF RFC 4572], which as its title states, describes *Connection-oriented media transport over the transport layer security (TLS) protocol in the session description protocol (SDP).*

Endpoints involved in a datagram transport layer security (DTLS) connection establishment (Note 1) indicate their identity by presenting authentication certificates as part of the DTLS handshake procedure. In order to associate the media streams with the connection and to prevent attacks, the endpoints provide a certificate fingerprint. If the presented certificate matches the received fingerprint, then the endpoint who sent the fingerprint is who it claims to be. [IETF RFC 4572] specifies a fingerprint attribute for this purpose.

NOTE 1 – Whether (or not) a *DTLS session* is established is dependent on if the establishment indicates the session as resumable. If used, there would then be a *resumable DTLS session* (or *semi-permanent DTLS session*) existing in parallel to the established DTLS connection.

[IETF RFC 4572] also defines the use of the "setup" and "connection" attributes defined by [IETF RFC 4145] to determine which of the endpoints initiates the DTLS handshake.

The support of DTLS in [ITU-T H.323] follows the same basic flow as described by [IETF RFC 4145]. That is a call signalling association is established between peer endpoints. The endpoints then exchange information regarding the media capabilities, transport and specific DTLS capabilities. They also indicate any DTLS extensions. For example, the use of DTLS for secure real-time transport protocol (SRTP) keying is indicated via a "use_srtp" extension. If the endpoints agree to use DTLS then they perform a DTLS handshake (Note 2) to initiate and authenticate a data stream. The endpoints use the fingerprint information to verify the authentication certificates provided in the DTLS handshake. If the certificates are verified, then the data flows. This is illustrated in Figure 1.

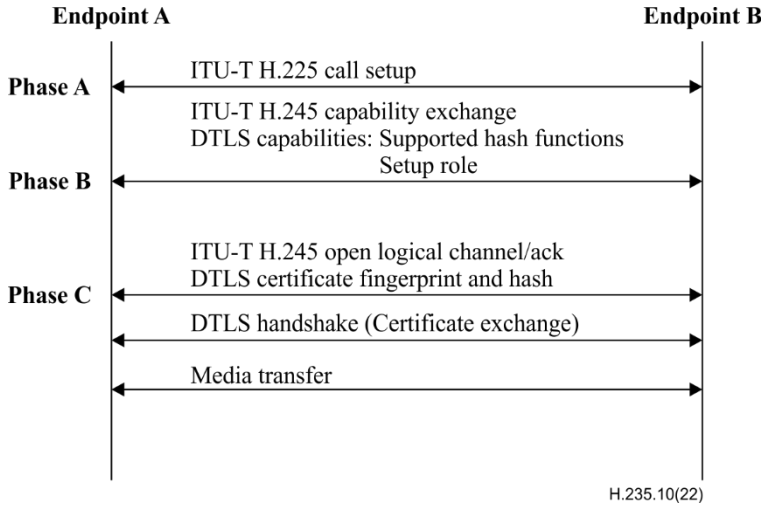

Figure 1 – Basic DTLS establishment flow

NOTE 2 – In more detail, this is a "DTLS full handshake" because a previous DTLS session does not exist, which might allow a DTLS abbreviated handshake.

7 Usage of DTLS

7.1 DTLS considerations

Depending on the protocol stack that DTLS occurs in there are different considerations for its implementation. Different DTLS procedures are applied based on where it occurs in a stack. For example, if a DTLS connection occurs within a stream control transmission protocol (SCTP)

association (SCTP/DTLS) [IETF RFC 6083] the implementation considerations are different to when an SCTP association occurs within a DTLS connection (DTLS/SCTP) [IETF RFC 8261].

Therefore, the exact DTLS procedures that should be applied to the media stream are determined by the indicated protocol in the ITU-T H.245 **MediaTransportType** or **DataProtocolCapability** element. Any definition of DTLS protocol in these elements shall specify a profile document that describes the operation of DTLS within that protocol stack. For example, clause B.2.2.7 of [ITU-T H.245] indicates that **sctp-dtls** is specified by [IETF RFC 6083].

These profile documents may also specify the use of the connection and set-up elements and the operation of other protocols in the stack.

A DTLS connection is tied to a particular transport address/port. DTLS uses the record layer in order to send encrypted data between peers. However, [IETF RFC 5764] on the use of DTLS to establish SRTP keys mandates that the record layer is not used and the underlying user datagram protocol (UDP) transport connection is used instead. Thus, if both the DTLS record layer (e.g., for SCTP data) and the UDP connection (for audio/video streams) are used for data, they shall be multiplexed on the same transport address/port and share the same DTLS connection for key negotiation.

7.2 DTLS parameter description

Information regarding the DTLS session is exchanged via the following parameters:

– **hashFunction** within the **DTLSSecurityCapability** contains the supported hash functions The value is encoded as per "hash-func" in the ABNF syntax as defined by clause 5 of [IETF RFC 4572].

– **setupInformation** within the **DTLSSecurityCapability** contains the set-up information used to determine which endpoint establishes the DTLS connection as defined by clause 4 of [IETF RFC 4572]. The value is encoded as per "role" in the ABNF syntax as defined by clause 4 of [IETF RFC 4145].

– **connectionInformation** within the **DTLSSecurityCapability** contains the connection information used to determine whether an existing or new connection is used for the DTLS connection as defined by clause 4 of [IETF RFC 4572]. The value is encoded as per "conn-value" in the augmented Backus-Naur form (ABNF) syntax as defined by clause 5 of [IETF RFC 4145].

– **fingerprint** within the **DTLSSecurityCapability** contains the fingerprint associated with the authentication certificates. The value is encoded as per "fingerprint" in the ABNF syntax as defined by clause 5 of [IETF RFC 4572].

– **extensionsType** within the **DTLSSecurityCapability** indicates which DTLS/TLS extensions are supported by the endpoint. The values are as per the Transport Layer Security (TLS) extensions Internet Assigned Numbers Authority (IANA) registry (http://www.iana.org/assignments/tls-extensiontype-values/). The "use_srtp" extension indicates that DTLS connection is used for SRTP keying. The resultant SRTP media flows use the same transport address/port as the DTLS connection.

The use of the DTLS security capability parameters in this Recommendation is limited to two-party bidirectional media streams where each source has a unique cryptographic key; support for multicast media streams or multipoint unicast streams is for further study.

7.3 DTLS parameter transport

7.3.1 DTLS Capabilities

The supported hash functions, set-up, extensions and connection information are carried in the **dtlsSecurityCapability** field of **encryptionAuthenticationAndIntegrity** in

H235SecurityCapability of the TerminalCapabilitySet **capabilityTable**. The **mediaCapability** field of the **H235SecurityCapability** is associated with the relevant receive or receiveAndTransmit capabilities. The fingerprint is not sent in the TerminalCapabilitySet exchange.

Different audio, video or data capabilities exchange may require the use of a single DTLS connection for key negotiation (e.g., SRTP and WebRTC channel using the same DTLS connection). In this case each of those capabilities shall include identical **dtlsSecurityCapability** fields. This may mean the common use of extensions (e.g., "use_srtp") that may only be applicable to one capability type but to the DTLS connection as a whole. This is also to avoid DTLS renegotiation.

NOTE – See clause 11 of [b-IETF RFC 8843]).

7.3.2 Fingerprint

The fingerprint associated with the authentication certificate of the OLC initiating endpoint is carried in the **dtlsSecurityCapability** field of **encryptionAuthenticationAndIntegrity** in **h235Media** of the **OpenLogicalChannel** (OLC) **forwardLogicalChannelParameters dataType** field. A single hash function used for the fingerprint shall also be present in the **dtlsSecurityCapability** field which is supported by both endpoints and chosen from the hash functions.

The fingerprint associated with the authentication certificate of the peer endpoint is carried in the **dtlsSecurityCapability** field of the **OpenLogicalChannelAck** (OLCAck). A single hash function used for the fingerprint shall also be present in the **dtlsSecurityCapability** field.

8 Procedures

The DTLS procedures described below shall only be used to negotiate security for two-party bidirectional media streams in situations where the ITU-T H.245 signalling channel is used. The ITU-T H.245 signalling channel may be protected by an encapsulating data-security protocol, e.g., IPsec [IETF RFC 4301] or TLS [IETF RFC 5246]. The exchange of DTLS crypto parameters using ITU-T H.245 messages shall provide the following functions:

1) Exchange and negotiation of DTLS capabilities: supported hash types, set-up role, extensions and whether an existing connection is to be used.
2) The exchange of fingerprints used to verify the authentication certificates used for the DTLS handshake for the channel.

8.1 Security capability exchange

The initiating endpoint indicates its DTLS capabilities as per clause 7.3.1. The initiating endpoint provides a list of hash functions (via the **hashFunction** field in **DTLSSecurityCapability)** that it supports to encode and decode authentication certificates. The peer endpoint replies with the sets of hash functions it supports. The initiating endpoint also sends the DTLS establishment role that it is willing to support (via the **setupInformation** field in **DTLSSecurityCapability)** as per clause 7.3.1 and clause 4.1 of [IETF RFC 4145]. The receiver then chooses based on the received roles, the role that the **TerminalCapabilitySet** initiator shall use for the DTLS connection.

The initiating endpoint provides the supported DTLS extensions in order to indicate the DTLS capabilities to the peer endpoint before establishing the connection. The peer endpoint may use this information when responding to the ITU-T H.245 capabilities exchange. The DTLS handshake is used to negotiate and agree on the set of DTLS extensions used for the connection

NOTE – There is a fundamental difference between H.323 and session initiation protocol (SIP) with regards to the establishment of the media stream. H.323 systems use the ITU-T H.245 master-slave determination procedures (clause C.2 of [ITU-T H.245]) to determine who is the master. Typically, the master is responsible for initiating connections, whereas in SIP/SDP for connections that require a handshake between

a master/slave the SDP a=setup attribute is used to determine the initiating party. Thus, problems occur when interworking between H.323 and SIP systems. It should be possible to open an end-to-end DTLS connection between the H.323 and SIP endpoints without the need to terminate the data stream (i.e., a gateway operates in a pass through mode). The procedures of this Recommendation allow the initiator of the DTLS handshake to be independent of the ITU-T H.245 master.

8.2 Logical channel initiation and fingerprint exchange

DTLS connections are fundamentally bidirectional in nature. For a logical channel utilising the DTLS record layer to transfer media, the master endpoint initiates a bidirectional OLC request containing the DTLS fingerprint and hash function as per clause 7.3.2. As per clause 6.2.8.2 of [ITU-T H.323] the bidirectional logical channel procedures (clause C.5 of [ITU-T H.245) are used to signal the initiation of a DTLS connection. For logical channels utilising DTLS only for key negotiation and another media transport type for transfer of media, a unidirectional OLC request is used.

In response to the OLC, the peer endpoint returns an OLCAck with its DTLS fingerprint and hash function.

In the case that an endpoint has indicated the use of a single DTLS connection for multiple audio, video, and/or data logical channel as per clause 7.3.1, identical values shall be returned in the OLCAcks related to those logical channels. The endpoint shall also use identical **portNumbers** to indicate that they share the same underlying transport.

The authentication certificates and the associated fingerprint used for the DTLS connection are generated according to the procedures specified in clauses 5 and 6 of [IETF RFC 4572]. The endpoint will use one of the hash functions negotiated through the security capability exchange outlined in clause 8.1. If the ITU-T H.245 connection is secured as per clause 8 then, as per clause 6.1 of [IETF RFC 4572], any certificate asserting a syntactically valid identity may be used. If the ITU-T H.245 signalling is not secured, then an appropriate identity shall be provided. This is FFS.

8.3 DTLS connection initiation

On reception of an OLC or OLCAck the endpoint that has been identified as the active endpoint for the DTLS connection initiation will initiate an outgoing DTLS connection to the peer to perform the DTLS handshake. During the handshake phase the certificates are exchanged as per [IETF RFC 6347] and clause 6.2 of [IETF RFC 4572]. The receipt of subsequent OLC/OLCAcks with the same **dtlsSecurityCapability** shall not initiate additional DTLS signalling.

As discussed in clause 7.1, different uses of DTLS may impose certain requirements for the DTLS handshake phase. The requirements are documented as part of profile document and are dependent on the transport, for example as per clause 4.7 of [IETF RFC 6083].

The endpoints then verify that the fingerprints of the certificates received during the DTLS handshake match the fingerprints received in the OLC or OLCAck messages. In this manner, the endpoints verify each other's credentials.

If the fingerprints do not match, the endpoint shall close the DTLS connection via a DTLS closure alert and then immediately close the logical channel.

Once the DTLS handshake is successfully completed and the credentials have been verified, data packets are transported in DTLS record layer "application_data" packets.

Some usages of DTLS (e.g., DTLS-SRTP) use alternate methods to transport data packets.

If the "use_srtp" extension has been negotiated via the DTLS handshake the endpoints shall follow the procedures of [IETF RFC 5764] to establish SRTP keying information and to send the SRTP/SRTCP data. In this case RTP and/or RTCP application data is protected via SRTP and not sent in the DTLS record layer "application_data" packets.

Whether the DTLS record layer or an alternate method is used is determined by the capabilities associated with the logical channel. For example, a **mediaTransportType** of UDP/DTLS/SCTP would indicate the use of the DTLS record layer, UDP would indicate the use of SRTP.

8.4 DTLS connection modification

Additional media may be added to an existing connection by utilising TCS / OLC signalling with an identical **dtlsSecurityCapability** field and **portNumber** (as appropriate) to the existing DTLS connection to avoid the DTLS renegotiation.

8.5 DTLS connection release

If the logical channel representing the DTLS connection is closed the security context is deleted and any application data shall stop flowing. That is, no packet shall be sent or received on the DTLS record layer. If SRTP keys have been negotiated via DTLS data flow shall cease on logical channels representing the SRTP/SRTCP streams.

Bibliography

[b-IETF RFC 8843] IETF RFC 8843 (2021), *Negotiating Media Multiplexing Using the Session Description Protocol (SDP)*.

[b-IETF tls-terms] IETF draft-guballa-tls-terminology-05 (2017), *Terminology related to TLS and DTLS*. https://datatracker.ietf.org/doc/html/draft-guballa-tls-terminology-05

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, 2022