International Telecommunication Union

ITU-T J.1004

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(08/2015)

SERIES J: CABLE NETWORKS AND TRANSMISSION OF TELEVISION, SOUND PROGRAMME AND OTHER MULTIMEDIA SIGNALS

Conditional access and protection – Renewable conditional access system

Specifications of authorization centre interfaces for renewable conditional access system

Recommendation ITU-T J.1004

Recommendation ITU-T J.1004

Specifications of authorization centre interfaces for renewable conditional access system

Summary

Recommendation ITU-T J.1004 specifies the authorization centre (AC) interfaces for a renewable conditional access system (RCAS) within the scope of ITU-T J.1001 that specifies the requirements of an RCAS. AC interfaces are the interfaces between a central authorization centre (CAC) and a conditional access module authentication subsystem (CASS) and between a distributed authorization centre (DAC) and a CASS.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T J.1004	2015-08-13	9	11.1002/1000/12569

* 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 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 J.1004

Specifications of authorization centre interfaces for renewable conditional access system

1 Scope

This Recommendation specifies authorization centre (AC) interfaces for a renewable conditional access system (RCAS). AC interfaces are the interfaces between a central authorization centre (CAC) and a conditional access module authentication subsystem (CASS) and between a distributed authorization centre (DAC) and a CASS.

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 J.1001] Recommendation ITU-T J.1001 (2012), *Requirements for renewable conditional access system.*

[ITU-T J.1002] Recommendation ITU-T J.1002 (2013), *Pairing protocol specification for renewable conditional access system.*

[ITU-T J.1003] Recommendation ITU-T J.1003 (2014), *Specification of network protocol for renewable conditional access system.*

[ITU-T X.509] Recommendation ITU-T X.509 (2008) | ISO/IEC 9594-8:2008, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*

[ITU-T X.690] Recommendation ITU-T X.690 (2008) | ISO/IEC 8825-1:2008, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 conditional access (CA) [b-ITU-T J.193]: The conditional granting of access to cable services and content based upon what service suite has been purchased by the customer.

3.1.2 descrambling [b-ITU-T J.93]: The process of reversing the scrambling function (see "scrambling") to yield usable pictures, sound, and data services.

3.1.3 entitlement control messages (ECMs) [b-ITU-T J.290]: An ECM is an encrypted message that contains access criteria to various service tiers and a control word (CW).

3.1.4 entitlement management messages (EMMs) [b-ITU-T J.290]: The EMM contains the actual authorization data and shall be sent in a secure method to each CPE device.

3.1.5 scrambling [b-ITU-T J.93]: The process of using an encryption function to render television and data signals unusable to unauthorized parties.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 DSC_ID: The identification value of the descrambler (DSC) having a size of 40 bytes.

3.2.2 CAM_ID: The identification value of the conditional access module (CAM) having a size of 8 bytes.

3.2.3 KeyPairingID: The value of the concatenation of CAM_ID and DSC_ID, i.e., CAM_ID||DSC_ID.

3.2.4 KPK: Key pairing key (KPK). The authorization centre (AC) generates the KPK if the KeyPairingID is valid.

3.2.5 RAND: A random number with 320 bits.

3.2.6 K_i: The pre-shared key having a size of 128 bits. The AC uniquely assigns three K_i to each CAM. K_i should be a generated random generation function.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AC	Authorization Centre
ASN	Abstract Syntax Notation
BER	Basic Encoding Rules
CACS	Conditional Access Client Software
CAM	Conditional Access Module
CASS	CAM Authentication Subsystem
CPE	Customer Premise Equipment
DAC	Distributed Authorization Centre
DOCSIS	Data Over Cable Service Interface Specification
DSC	Descrambler
HMAC	Hash-based Message Authentication Code
KPK	Key Pairing Key
MSB	Most Significant Bit
PRF	Pseudo Random number generation Function
PRNG	Pseudo Random Number Generator
RCAS	Renewable Conditional Access System
STB	Set Top Box

5 Conventions

In this Recommendation:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "**is prohibited from**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

In the body of this Recommendation and its annexes, the words *shall*, *shall not*, *should*, and *may* sometimes appear, in which case they are to be interpreted, respectively, as *is required to*, *is prohibited from*, *is recommended*, and *can optionally*. The appearance of such phrases or keywords in an appendix or in material explicitly marked as *informative* are to be interpreted as having no normative intent.

6 Overview of RCAS authorization centre interfaces

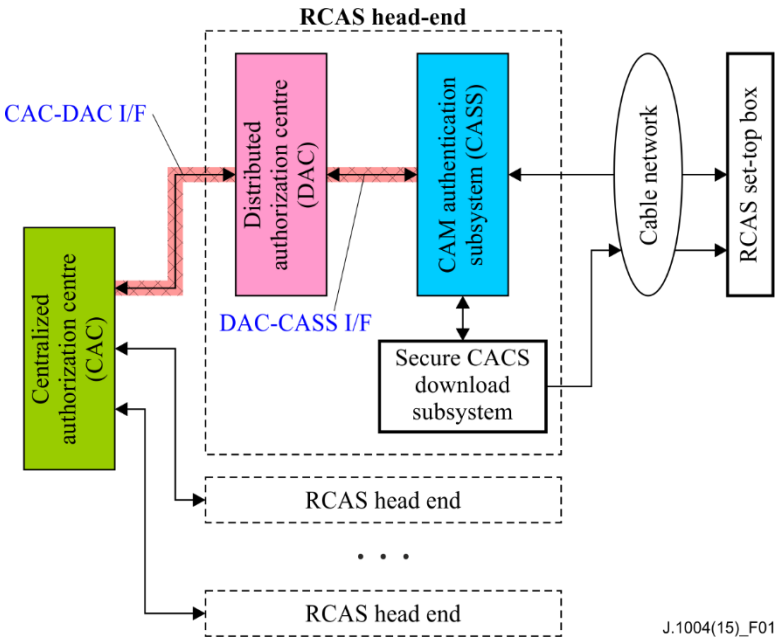

Figure 1 – CAC-DAC and DAC-CASS interfaces in RCAS

Renewable conditional access system (RCAS) is a new paradigm technology for renewing conditional access client software (CACS) by securely downloading a new CACS through the digital cable two-way environment. There are three relevant Recommendations for RCAS: [ITU-T J.1001], [ITU-T J.1002] and [ITU-T J.1003]. [ITU-T J.1001] contains architectural, functional and security requirements of RCAS. [ITU-T J.1002] and [ITU-T J.1003] are Recommendations for the RCAS pairing specification and the RCAS network specification, respectively.

One of the important architectural subsystems in RCAS is the authorization centre (AC) as described in [ITU-T J.1001]. The AC plays a very important role for mutual authentication between the RCAS head end and the conditional access module (CAM) in the RCAS set-top box (STB).

Typically a multiple service operator (MSO) has multiple RCAS head ends since one RCAS head end cannot cover all service areas which are distant from each other. Therefore the RCAS AC should be separated with a centralized authorization centre (CAC) and a distributed authorization centre

(DAC) as shown in Figure 1 to efficiently manage the authentication process of the RCAS STBs including the CAM.

As shown in Figure 1, an MSO has only one CAC and locates one DAC in each of the RCAS head end. Therefore the interface architecture of a CAC and a DAC is 1:N, and that of a DAC and a CASS is 1:1.

7 Specifications DAC-CASS interface

The basic role of the DAC is issuing ITU-T X.509 certificates of RCAS headend servers but it also includes more specific functions as follows:

– Generating a unique identification number for each RCAS headend server

– Validating pairing between the CAM and the descrambler [ITU-T J.1002]

– Managing parameters needed for authentication of RCAS STBs

– Join/leave processing for retail and leased RCAS STBs.

There are two types of messages for the interface between the DAC and the CASS, these are the AMFB_TRANS_INFO and AMFB_AUTH_INFO_RECV messages. The sequence diagram for these two message types is shown in Figure 2.

Figure 2 – Sequence diagram for DAC-CASS interface messages

The message format for the DAC-CASS interface is shown in Figure 3. The messages are encoded as ASN.1 data and the most significant bit (MSB) is transmitted first.

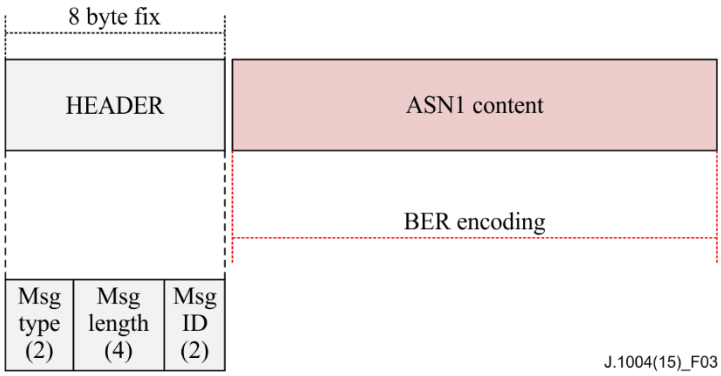

Figure 3 – AC interface message format

7.1 AMFB_TRANS_INFO

The function of AMFB_TRANS_INFO is used for delivering a JOIN request from a CASS to a DAC after the JOIN request is received from the RCAS STB to the CASS as shown in Figure 2. The message type value for AMFB_TRANS_INFO is 0x0401.

The ASN.1 syntax notation for AMFB_TRANS_INFO is shown below:

```
-- ============================================================
-- AMFB_TRANS_INFO
-- ============================================================

KeyReqMsgContent ::= SEQUENCE
{
  cASSID                  OCTET STRING (SIZE (4)),

  keyPairingID             OCTET STRING (SIZE (48))
}
```

– **cASSID** : The value of ID for the CASS

– **keyPairingID**: This is the key pairing ID which is sent from the CAM and generated by concatenating 'Descrambler ID' and 'CAM ID'.

7.2 AMFB_AUTH_INFO_RECV

The function of AMFB_TRANS_INFO_RECV is used for delivering security parameters from the DAC to the CASS as shown in Figure 2. These security parameters are generated by utilizing K_i and the operator variant algorithm configuration field (OP) values of the RCAS STB, see [ITU-T J.1003]. The message type value for AMFB_AUTH_INFO_RECV is 0x0400.

The ASN.1 syntax notation for AMFB_AUTH_INFO_RECV is shown below:

```
-- ============================================================
-- AMFB_AUTH_INFO_RECV
-- ============================================================

KeyRspMsgContent ::= SEQUENCE
{

  -- Authentication Resut, success = TRUE, fail = FALSE
  auth-Rst                BOOLEAN (TRUE),

  rAND-DAC                RandDAC,

  kC                      Kc,

  kPK                     OCTET STRING (SIZE (20)),

  sign-KPK                OCTET STRING (SIZE (128))

}

RandDAC  ::= SEQUENCE
{
  rAND-DAC-1                 OCTET STRING (SIZE (16)),
  rAND-DAC-2                 OCTET STRING (SIZE (16)),
  rAND-DAC-3                 OCTET STRING (SIZE (16))
}

Kc  ::= SEQUENCE
{
  kc-1                    OCTET STRING (SIZE (8)),
  kc-2                    OCTET STRING (SIZE (8)),
  kc-3                    OCTET STRING (SIZE (8))
}
```

– **Auth-Rst**: The authentication result for RCAS STB. If the authentication process is successful, the value is TRUE. Otherwise the value should be FALSE.

– **rAND-DAC**: This is the RAND-DAC which is used for one of the input parameters of the session key generation function. The DAC randomly generates a RAND-DAC per RCAS STB and the RCAS STB manufacturer inserts the value of the RAND-DAC into the CAM of the RCAS STB.

– **kC**: This is the Kc which is used for one of the input parameters of the session key generation function. The Kc is generated with the random number generation function using the Ki and RAND-DAC as input parameters. The CAC randomly generates a Ki per RCAS STB and the RCAS STB manufacturer inserts a Ki into the CAM of the RCAS STB, see [ITU-T J.1003].

– **kPK**: This is the key pairing key (KPK). For a definition of the KPK, see [ITU-T J.1003].

– **sign-KPK**: This is the value of the digital signature of the KPK [ITU-T J.1003].

8 Specifications for a CAC-DAC interface

The message types for a CAC-DAC interface are defined as shown the below:

Direction	Message name	Message type
DAC → CAC	JOIN_ INFO_REPORT	0X0501
CAC → DAC	ACK_JOIN_ INFO_REPORT	0X0502
DAC → CAC	LEAVE_ INFO_REPORT	0X0504
CAC → DAC	ACK_LEAVE_ INFO_REPORT	0X0505
DAC → CAC	CERTIFICATE_STATE_UPDATE	0X0521
CAC → DAC	ACK_CERTIFICATE_STATE_UPDATE	0X0522
CAC → DAC	CERTIFICATE_ISSUE_TRANSFER	0X0511
DAC → CAC	ACK_CERTIFICATE_ISSUE_TRANSFER	0X0512

The message format for a CAC-DAC interface is shown in Figure 3. The messages are encoded as ASN.1 data and the MSB is transmitted first.

8.1 JOIN_INFO_REPORT

When a DAC sucessfully validates a join request from a retail RCAS STB via a CASS in the RCAS head end, the DAC delivers the information regarding the retail RCAS STB and RCAS head end to the CAC through a JOIN_INFO_REPORT message. The received information of a retail RCAS STB in the CAC is delivered to all other DACs in different RCAS head end using a CERTIFICATE_STATE_UPDATE message.

The ASN.1 syntax notation for a JOIN_INFO_REPORT is shown below:

```
-- ============================================================
-- JOIN_INFO_REPORT
-- ============================================================

JoinInfoRptMsgContent ::= SEQUENCE
{
  dACID                    OCTET STRING (SIZE (4)),

  cASSID                   OCTET STRING (SIZE (4)),

  cAMID                    OCTET STRING (SIZE (40)),

  dSCID                    OCTET STRING (SIZE (8))
}
```

8.2 ACK_JOIN_INFO_REPORT

A CAC uses an ACK_JOIN_INFO_REPORT message to reply with the process result of a JOIN_INFO_REPORT message to a DAC. The result will be TRUE only if the CAC successfully receives and processes the JOIN_INFO_REPORT. Otherwise, the result will be FALSE.

The ASN.1 syntax notation for an ACK_JOIN_INFO_REPORT is shown below:

```
-- ============================================================
-- ACK_JOIN_INFO_REPORT
-- ============================================================

AckJoinInfoRptMsgContent ::= SEQUENCE
{

  join-Proc-Rst               BOOLEAN (FALSE)

}
```

8.3 LEAVE_INFO_REPORT

When a DAC sucessfully validates a leave request from a retail RCAS STB via a CASS in the RCAS head end, the DAC delivers the information regarding the retail RCAS STB and RCAS head end to the CAC through a LEAVE_INFO_REPORT message. The recevied information of a retail RCAS STB in the CAC is delivered to all other DACs in different RCAS head end using a CERTIFICATE_STATE_UPDATE message.

The ASN.1 syntax notation for a LEAVE_INFO_REPORT is shown below:

```
-- ================================================================
-- LEAVE_INFO_REPORT
-- ================================================================

LeaveInfoRptMsgContent ::= SEQUENCE
{
  dACID                    OCTET STRING (SIZE (4)),

  cASSID                   OCTET STRING (SIZE (4)),

  cAMID                    OCTET STRING (SIZE (40)),

  dSCID                    OCTET STRING (SIZE (8))
}
```

8.4 ACK_LEAVE_INFO_REPORT

A CAC uses an ACK_LEAVE_INFO_REPORT message to reply with the process result of a LEAVE_INFO_REPORT message to a DAC. The result will be TRUE only if the CAC successfully receives and processes the LEAVE_INFO_REPORT. Otherwise, the result will be FALSE.

The ASN.1 syntax notation for an ACK_LEAVE_INFO_REPORT is shown below:

```
-- ================================================================
-- ACK_LEAVE_INFO_REPORT
-- ================================================================

AckLeaveInfoRptMsgContent ::= SEQUENCE
{

  leave-Proc-Rst            BOOLEAN (FALSE)

}
```

8.5 CERTIFICATE_STATE_UPDATE

After a CAC receives a JOIN_INFO_REPORT or a LEAVE_INFO_REPORT message from a DAC, it updates the database for a retail RCAS STB's status based on the received message. Then the CAC sends out the relevant information to other RCAS headend DACs using a CERTIFICATE_STATE_UPDATE.

Then each DAC that receives a CERTIFICATE_STATE_UPDATE, updates its database based on the information from the received CERTIFICATE_STATE_UPDATE message so that all of the DACs have the same database information for a retail RCAS STB.

The parameters in a CERTIFICATE_STATE_UPDATE are database UPDATE queries.

The ASN.1 syntax notation for a CERTIFICATE_STATE_UPDATE is shown below:

```
-- ================================================================
-- CERTIFICATE_STATE_UPDATE
-- ================================================================

CertStateUpdateMsgContent ::= SEQUENCE
{

  cAMQuery                  OCTET STRING (SIZE (1024)),

  dSCQuery                  OCTET STRING (SIZE (1024)),

  pAIRQuery                 OCTET STRING (SIZE (1024))

}
```

8.6 ACK_CERTIFICATE_STATE_UPDATE

A DAC uses an ACK_CERTIFICATE_STATE_UPDATE message to reply with the process result of a CERTIFICATE_STATE_UPDATE message to a CAC. The result will be TRUE only if the DAC successfully receives and processes the CERTIFICATE_STATE_UPDATE. Otherwise, the result will be FALSE.

The ASN.1 syntax notation for ACK_CERTIFICATE_STATE_UPDATE is shown below:

```
-- ================================================================
-- ACK_LEAVE_INFO_REPORT
-- ================================================================

AckLeaveInfoRptMsgContent ::= SEQUENCE
{

  leave-Proc-Rst            BOOLEAN (FALSE)

}
```

8.7 CERTIFICATE_ISSUE_TRANSFER

A CAC uses a CERTIFICATE_ISSUE_TRANSFER when it needs to deliver retail RCAS STB certificates information to a DAC on-line. The explanations for each parameter are as follows:

– NextFlag: If this message is for the last certificate to be delivered, the CAC sets this parameter as FALSE. Otherwise, the value should be TRUE.

– SubFolderPath: The delivered certificate should be stored in the folder with the path written in this parameter.

– FileLength: The length of the certificate delivered.

– FileName: The name of the certificate delivered.

The ASN.1 syntax notation for CERTIFICATE_ISSUE_TRANSFER is shown below:

```
-- ================================================================
-- CERTIFICATE_ISSUE_TRANSFER
-- ================================================================

CertIssueTransfereMsgContent ::= SEQUENCE
{

  nextFlag                  BOOLEAN (FALSE),

  subFloderPath             OCTET STRING (SIZE (1024)),

  fileLength                INTEGER,

  fileName                  OCTET STRING (SIZE (1024))

}
```

8.8 ACK_CERTIFICATE_ISSUE_TRANSFER

A DAC uses an ACK_CERTIFICATE_ISSUE_TRANSFER message to reply with the process result of a CERTIFICATE_ISSUE_TRANSFER message and the relevant certificate to a CAC. It must be noted that the DAC should send this message to the CAC only if the value of the parameter NextFlag is FALSE. For instance, if the CAC is supposed to deliver 10 CERTIFICATE_ISSUE_TRANSFER messages to a DAC, the DAC should reply with an ACK_CERTIFICATE_ISSUE_TRANSFER message after 10 CERTIFICATE_ISSUE_TRANSFER messages are received and the value of NextFlag is FALSE.

The ASN.1 syntax notation for an ACK_CERTIFICATE_ISSUE_TRANSFER is shown below:

```
-- ================================================================
-- ACK_CERTIFICATE_ISSUE_TRANSFER
-- ================================================================

AckCertIssueTransfereMsgContent ::= SEQUENCE
{

  dACID                     OCTET STRING (SIZE (4)),

  cert-Cert-Trans-Rst           BOOLEAN (FALSE)

}

END
```

Bibliography

[b-ITU-T J.93] Recommendation ITU-T J.93 (1998), *Requirements for conditional access in the secondary distribution of digital television on cable television systems*.

[b-ITU-T J.122] Recommendation ITU-T J.122 (2007), *Second-generation transmission systems for interactive cable television services – IP cable modems*.

[b-ITU-T J.128] Recommendation ITU-T J.128 (2008), *Set-top gateway specification for transmission systems for interactive cable television services*.

[b-ITU-T J.193] Recommendation ITU-T J.193 (2004), *Requirements for the next generation of set-top-boxes*.

[b-ITU-T J.290] Recommendation ITU-T J.290 (2006), *Next generation set-top box core architecture*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
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	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
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 and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2015