EAP-based security signalling protocol architecture for network attachment

ITU-T Recommendation Q.3201
<table>
<thead>
<tr>
<th>Topic</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE</td>
<td>Q.1–Q.3</td>
</tr>
<tr>
<td>INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING</td>
<td>Q.4–Q.59</td>
</tr>
<tr>
<td>FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN</td>
<td>Q.60–Q.99</td>
</tr>
<tr>
<td>CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS</td>
<td>Q.100–Q.119</td>
</tr>
<tr>
<td>SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2</td>
<td>Q.120–Q.499</td>
</tr>
<tr>
<td>DIGITAL EXCHANGES</td>
<td>Q.500–Q.599</td>
</tr>
<tr>
<td>INTERWORKING OF SIGNALLING SYSTEMS</td>
<td>Q.600–Q.699</td>
</tr>
<tr>
<td>SPECIFICATIONS OF SIGNALLING SYSTEM No. 7</td>
<td>Q.700–Q.799</td>
</tr>
<tr>
<td>Q3 INTERFACE</td>
<td>Q.800–Q.849</td>
</tr>
<tr>
<td>DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1</td>
<td>Q.850–Q.999</td>
</tr>
<tr>
<td>PUBLIC LAND MOBILE NETWORK</td>
<td>Q.1000–Q.1099</td>
</tr>
<tr>
<td>INTERWORKING WITH SATELLITE MOBILE SYSTEMS</td>
<td>Q.1100–Q.1199</td>
</tr>
<tr>
<td>INTELLIGENT NETWORK</td>
<td>Q.1200–Q.1699</td>
</tr>
<tr>
<td>SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000</td>
<td>Q.1700–Q.1799</td>
</tr>
<tr>
<td>SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)</td>
<td>Q.1900–Q.1999</td>
</tr>
<tr>
<td>BROADBAND ISDN</td>
<td>Q.2000–Q.2999</td>
</tr>
<tr>
<td>SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN</td>
<td>Q.3000–Q.3999</td>
</tr>
<tr>
<td>General</td>
<td>Q.3000–Q.3029</td>
</tr>
<tr>
<td>Network signalling and control functional architecture</td>
<td>Q.3030–Q.3099</td>
</tr>
<tr>
<td>Network data organization within the NGN</td>
<td>Q.3100–Q.3129</td>
</tr>
<tr>
<td>Bearer control signalling</td>
<td>Q.3130–Q.3179</td>
</tr>
<tr>
<td><strong>Signalling and control requirements and protocols to support attachment in NGN environments</strong></td>
<td><strong>Q.3200–Q.3249</strong></td>
</tr>
<tr>
<td>Resource control protocols</td>
<td>Q.3300–Q.3369</td>
</tr>
<tr>
<td>Service and session control protocols</td>
<td>Q.3400–Q.3499</td>
</tr>
<tr>
<td>Service and session control protocols – supplementary services</td>
<td>Q.3600–Q.3649</td>
</tr>
<tr>
<td>NGN applications</td>
<td>Q.3700–Q.3849</td>
</tr>
<tr>
<td>Testing for NGN networks</td>
<td>Q.3900–Q.3999</td>
</tr>
</tbody>
</table>

For further details, please refer to the list of ITU-T Recommendations.
ITU-T Recommendation Q.3201

EAP-based security signalling protocol
architecture for network attachment

Summary

ITU-T Recommendation Q.3201 describes the security signalling requirements and protocol architecture for supporting access security aspects of network attachment procedure in a next generation network (NGN). Basic threats and security requirements for the attachment of NGN access networks are analysed, and a model of an extensible authentication protocol (EAP)-based security signalling protocol architecture accommodating heterogeneous multi-links in the next generation network access environment is presented. Based on it, three feasible scenarios for authentication signalling in NGN network attachment control functions are developed.

Source

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

© ITU 2008

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.
## CONTENTS

<table>
<thead>
<tr>
<th>Page</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Scope ........................................................................................................................ .... 1</td>
</tr>
<tr>
<td>1.1</td>
<td>Relationship.................................................................................................... 1</td>
</tr>
<tr>
<td>2</td>
<td>References................................................................................................................... .. 1</td>
</tr>
<tr>
<td>3</td>
<td>Abbreviations............................................................................................................ 2</td>
</tr>
<tr>
<td>4</td>
<td>Threats on access networks ..................................................................................... 3</td>
</tr>
<tr>
<td>5</td>
<td>Conventions ............................................................................................................... 4</td>
</tr>
<tr>
<td>6</td>
<td>Security requirements for access networks.......................................................... 4</td>
</tr>
<tr>
<td>7</td>
<td>Signalling protocol architecture for authentication .................................................. 5</td>
</tr>
<tr>
<td>7.1</td>
<td>Basic authentication model............................................................................. 7</td>
</tr>
<tr>
<td>7.2</td>
<td>EAP-based authentication architecture in access networks............................ 8</td>
</tr>
<tr>
<td>7.3</td>
<td>EAP authentication model........................................................................... 9</td>
</tr>
<tr>
<td>7.4</td>
<td>Integrated authentication model in NGN ....................................................... 9</td>
</tr>
<tr>
<td>7.5</td>
<td>Authentication scenarios based on network architecture .............................. 10</td>
</tr>
<tr>
<td>Bibliography .............................................................................................................. 14</td>
<td></td>
</tr>
</tbody>
</table>
ITU-T Recommendation Q.3201

EAP-based security signalling protocol architecture for network attachment

1 Scope

This Recommendation provides the basic security framework protocol architecture to support network attachment in NGN environments. This Recommendation also provides some threats and security requirements related to the signalling and control for network attachment.

The goal of this Recommendation is to identify security requirements for access networks and to define an EAP-based security protocol architecture for network access attachment. The main focus of this Recommendation is on an EAP-based security signalling protocol architecture for authentication and authorization in the network attachment system of NGN.

This Recommendation incorporates the overall context of related standards, on the issue of network security protocol, from IETF, IEEE and ITU-T.

1.1 Relationship

Work for this Recommendation is based upon the context of [ITU-T Y.2701] and [ITU-T Y.2012]; this Recommendation complies with the security requirements and guidelines specified in [ITU-T Y.2701], and considers the compatibility with the functional architecture in [ITU-T Y.2012].

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.


3 Abbreviations

This Recommendation uses the following abbreviations:

AAA Authentication, Authorization and Accounting
AKA Authentication and Key Agreement
ANI Access Network Interface
AP Access Point
AR-FE Acces Relay Functional Entity
AS Authentication Server
BB Broadband
DoS Denial of Service
EAP Extensible Authentication Protocol
EAPoL Extensible Authentication Protocol over Local Area Network
EP Enforcement Point
FE Functional Entity
GW Gateway
HSS Home Subscriber Server
ID Identity
IMS Internet Protocol Multimedia Subsystem
4 Threats on access networks

This clause discusses some possible threats on the authentication, defined in [IETF RFC 4016], of the access network.

Success or failure indications

When a client accesses the network, an attacker can fool the client to fail to be authenticated using a false authentication failure message. The attacker may launch a denial of service (DoS) attack and break the authentication signalling by sending a number of false failure messages. If the communication channel between the customer device and the authenticator is not protected by a security association, the attacker can easily make false failure messages. The customer device and the authenticator can prevent this attack by using the authentication keys established in the mutual authentication procedure. Success or failure indication messages shall be encrypted or decrypted using the authentication keys.
Man-in-the-middle attack (MITM)
An attacker can claim to be the customer device or the authenticator between the real customer device and the real authenticator. Using the man-in-the-middle (MITM) attack, the attacker can steal the security association between the real customer device and the real authenticator. If the attacker is successful in the man-in-the-middle (MITM) attack, the attacker can sniff all the messages and insert a spoof message channel between the real customer device and the real authenticator. The attacker, therefore, gains a capability to execute all different kinds of attacks later.

Replay attack
An attacker can replay the valid authentication messages to cause false failures or success. The customer device and the authenticator can be protected from this attack by encrypting the message with a sequence number or time stamp.

Device identifier attack
The authenticator identifies the customer device using a device identifier. In case of successful authentication, the client can send the packet with the device identifier because the authenticator controls the authenticated traffic using the device identifier. However, the attacker can also send the packet using the device identifier without the authentication procedure. This attack can be prevented by using the security association between the customer device and the authenticator.

Client leaving the network
When the client is about to leave the access network, it should inform the authenticator of the service termination before it leaves, returning the allowed resources to the authentication client. If the customer device leaves the network without a notification, the attacker may pretend to be the client and use the network or transmit a disconnect message.

Service theft
An attacker can steal the network access service by pretending to be the authenticated client. After the client is successfully authenticated, the enforcement point will control traffic to prevent unauthorized traffic into the network. The filtering will be based on the IP and MAC addresses. Any attacker who can spoof the IP and MAC addresses in the packets can launch a service-theft attack easily. This attack can be prevented using per-packet protection with the security association between the customer device and the authenticator.

Denial of service (DoS) attack
Since the access network is vulnerable to many kinds of DoS attacks targeting the authentication agent or authenticator, the protocol should be designed to prevent DoS attacks. An attacker can perform a focused attack on the victim authenticator using a bunch of authentication requests. Since the authenticator may allocate resources to maintain the state information of the authentication client during the authentication process, the attacker can deplete the resources of the authenticator or authentication server.

5 Conventions
None.

6 Security requirements for access networks
This clause discusses the security requirements for the access network defined in [IETF RFC 4058].
Multi-access

The authentication procedure should support authentication clients with multiple interfaces, and networks on multi-access links. The authentication procedure should consider three different cases such that the authentication client may have multiple network interfaces, that the access network has not only a one-hop router but also a two- or three-hop router, or that the authentication client is not only using a point-to-point link but also multipoint links.

Disconnect indication

The authentication procedure should not assume that the link is connection-oriented. Link protocol may or may not support the disconnect indication, which helps to return the resources after the end of the service. The authentication protocol must be able to protect the disconnect messages to prevent a DoS attack.

Secure channel

The authentication protocol must consider protecting the communication channel between the authentication client and authenticator. Through the secure channel, the authentication protocol can protect the resource against many attacks such as eavesdropping, spoofing or replay attacks.

The authentication protocol can obtain a secure channel by mutual authentication as well as the security association shared between the authentication client and authenticator.

Performance

The authentication protocol must be designed to have minimum latency and overhead messages for network access.

Denial of service attacks

The authentication protocol can prevent many kinds of DoS attacks. Such attacks will incur the spending of resources of the authenticator and preventing network access by legitimate clients.

Client identity privacy

A client in a visiting network may want to hide its identity for privacy reasons. The signalling of the access network can support the identity privacy by hiding the real identity of the client.

Fast handover support

When the customer device moves from the current access point to another, the customer device should re-authenticate through the new access point after changing the attachment point. This means extra delay for the re-authentication procedure. The authentication procedure should support fast handover for the real-time service user.

Roaming support

When moving into another administrative domain after changing the attachment point, a customer device authenticated by the current administrative domain should be re-authenticated in the new administrative domain. Cooperation among administrative domains is required for re-authenticating the mobile user. Therefore, the authentication procedure should support the roaming of the authentication context between administrative domains.

7 Signalling protocol architecture for authentication

The network attachment control functions (NACFs) defined in [ITU-T Y.2012] provides the registration function at the access level and initialization of the end-user functions for accessing to the NGN services. The functions include providing network level identification/authentication, managing the IP address space of the access network, and authenticating the access signalling
sessions. The functions also announce the contact point of the NGN service/application functions to the end user.

Figure 1 – Overview of NGN architecture

This Recommendation defines the authentication and authorization part of the network attachment control functions in the transport control functions. The transport functions include access network functions, edge functions, core transport functions, and gateway functions.

This Recommendation provides the following functionalities:

- Authentication occurring at the IP layer before or during the IP address allocation procedure.
- Authorization of network access, based on the user profile.

Authentication and authorization functions allow the user's network access and the use of network resources using user information from the user profile function. In other words, these functions authenticate users who want to access the network and check the user's ID and authority.

Figure 2 shows the network attachment control functions part of the NGN generalized functional architecture defined in [ITU-T Y.2012]. The scope of this Recommendation covers T-11 (TAA-FE), T-12 (TUP-FE), and T-14 (AM-FE).
The transport authentication and authorization functional entity (TAA-FE) provides authentication and authorization functions at the transport stratum.

The detailed functions are as follows:

a) TAA-FE shall need to specify how users/terminals are identified in the access networks. The identification function is the first step in the mobility management process and is used for authentication, authorization and accounting (AAA) of users/terminals.

b) TAA-FE should support the common authentication, authorization and accounting (AAA), and security schemes.

The authentication and authorization function should be coordinated with the commonly used AAA and security schemes to be authenticated, authorized, accounted and secured for the services.

7.1 Basic authentication model

The basic authentication model in NGN must include all of the different kinds of authentication at each level. Figure 3 describes the detail of the authentication functions in NGN. Authentication functions may support three different levels of authentication: link-level authentication, network-level authentication, and user-level authentication. In particular, the link-level authentication is performed by access network functions directly connected to the user devices. Access network functions can identify the access device using a device identifier such as the SSID or MAC address associated with authentication information. On the other hand, the network-level authentication function can identify the network level address, such as the IP address, associated with authentication information. Finally, the user-level authentication function may use the user ID or user profile information for authentication.
7.2 EAP-based authentication architecture in access networks

The authentication functions in NGN should support many different kinds of authentication procedure for heterogeneous access networks. Figure 4 describes the detail of the EAP-based authentication functions in NGN. The authentication functions in the transport stratum may support the link-level authentication, network-level authentication, or user-level authentication.

7.2.1 Link-level authentication

To support different authentication procedures for many kinds of access networks, access network functions shall include the existing link-level authentication protocol used in [IEEE 802.11i] and [3GPP TS 33.102]. Access network functions can identify the access device using the device identifier such as SSID or MAC address.

7.2.2 Network-level authentication

The network-level authentication function may use the PANA protocol [IETF RFC 4016] to carry authentication information for network access. The PANA protocol allows clients to authenticate themselves to the access network using IP. Such a protocol would allow a client to interact with TAA-FE to gain access without the need to understand any specific AAA protocols that are in use at the site. It would also allow such interactions to take place without a link-layer specific mechanism. PANA would be applicable to both multi-access and point-to-point links. It would provide support for various authentication methods, dynamic service provider selection, and roaming clients.

The network-level authentication function also includes AM-FE (AAA client function) to communicate with TAA-FE (AAA server function) for user authentication using DIAMETER [IETF RFC 3588] or RADIUS [IETF RFC 2865]. Since the network-level authentication function is related to the network address, NACF may include the IP address space of the access network.

7.2.3 User-level authentication

Since it manages the user information for each user, the AAA server provides NACF with the user authentication function during the authentication procedure. TAA-FE communicates with AM-FE in NACF for authenticating the user using DIAMETER or RADIUS protocol.
7.3 EAP authentication model

The EAP protocol defines an authentication framework that supports various authentication methods. EAP runs on the peer and authentication server via authenticator. EAP is directly transported over data link layers such as [b-IEEE 802] and point-to-point protocol (PPP). However, due to the feature of link dependency, the EAP protocol requires a lower layer such as EAPoL, [b-IEEE 802.1x], or [IEEE 802.11i]. Figure 5 describes the EAP multiplexing model. The EAP method layer includes an authentication algorithm. The EAP peer and authenticator have functionalities as authentication client and authenticator, respectively. The EAP layer performs the delivery of the EAP messages. The lower layer transmits or receives the EAP frames between the peer and the authenticator. Since the link layer consists of various link protocols, EAP requires various lower layers for each link protocol.

![Figure 5 – EAP forwarding model](Q.3201(07)_F06)

7.3.1 Lower layer requirements

The EAP requires a lower layer for reliable message delivery, error detection and ordering message as follows:

- Since it does not know that the peer receives the message from the authenticator, EAP requires a reliable channel between the peer and the authenticator.
- EAP does not guarantee that the EAP messages are delivered to the destination without error. Thus, EAP needs an error detection function from the lower layer.
- EAP messages may be changed in order or duplicated for any reason. Thus, EAP requires duplicate detection and ordering to guarantee correct operations.
- The lower layer does not know whether or not the upper layer includes authentication protocol. EAP requires an indication of the authentication protocol.

7.4 Integrated authentication model in NGN

Due to different access technologies, EAP lower layers are developed for each link protocol. Since the various authentication protocols are difficult to control by one management node, the NGN architecture requires an integrated authentication model. The objectives of the authentication model are as follows:

- To unify the authentication point for various interfaces.
- To support an authenticating peer indirectly connected to the authenticator.
- To support fast handover without authentication in the same administration domain.
- To support vertical handover without authentication in the same administration domain.
Figure 6 shows an integrated authentication model, which is controlled by an authenticator. The peer sends authentication information to the enforcement point, which in turn forwards it to the authenticator. This architecture helps the authenticator manage the authentication procedure.

![Integrated authentication model](Q.320107_F06)

**Figure 6 – Integrated authentication model**

Figure 7 depicts an integrated authentication model in NGN. It is assumed that the network attachment control functions are the authenticator and authentication server, and the access network functions are the enforcement points. The access network performs filtering of data packets allowing only the authenticated packets. After successful authentication of the end-user function, the access network functions allow the packets from the end-user function to enter into the access network.

![Integrated authentication model in NGN](Q.320107_F07)

**Figure 7 – Integrated authentication model in NGN**

7.5 Authentication scenarios based on network architecture

7.5.1 In case the mobile nodes are directly connected to the access network functions

Legacy end-user functions still have the EAP module operated on the link layer. Although EAP runs on the link layer between access network functions (e.g., AR-FE) and end-user functions, NGN has an IP-based transport protocol. Due to this reason, EAP over the link layer is not directly transported in the NGN architecture. For delivery of the EAP message in NGN, the transformation of the lower layer is required in the access network functions. Access network functions have the transformation function, which changes the lower layer of the link layer such as EAPoL.
[IEEE 802.11i] to the lower layer of the network layer such as PANA. The reference point T-U1 allows the end-user functions to request AR-FE for the delivery of the EAP messages over the link layer. TC-T1 allows AR-FE to request AM-FE for the transport of EAP messages over the network layer.

Figure 8 – Authentication architecture for EAP over the link layer

Access link technologies are developed in several link protocols such as the Ethernet and [b-IEEE 802.11]. The lower layer between the end-user function and access network functions depend on the link protocol. In the case of Ethernet, EAPoL shall be necessary for the delivery of the EAP message. When PPP is used for the link protocol, the authentication control option is also required to transport the message. Although the lower layers run directly on the link layer, the access network functions will change the link protocol with the lower layer. The access network functions will use the network layer as the transport protocol of EAP, and EAP also requires a lower layer on the network layer such as PANA. To transform the lower layer, the access network functions will do mapping of the lower layer protocols on each side. Thus, EAP messages are transported over IP from the access network functions to AM-FE. Since AM-FE is the authenticator, AM-FE will change the EAP peer layer to the EAP authenticator layer. The EAP message between AM-FE and TAA-FE will be delivered by an AAA protocol such as DIAMETER or RADIUS.

Figure 9 – EAP forwarding model for EAP over the link layer
7.5.2 In case the mobile nodes are indirectly connected to the access network functions via a gateway

The end-user functions may be connected indirectly to the access network functions (e.g., AR-FE) via the gateway such as in home networks. If EAP messages are transferred to the access network functions via the gateway, the lower layer on the link protocol should be changed to the lower layer specific for the link protocol between the gateway and access network functions. Thus, EAP messages between the end-user functions and the gateway are transported on the link layer, and the EAP messages between the gateway and the access network functions are delivered on the network layer.

Figure 10 – Authentication architecture for EAP over the link layer via gateway

Figure 11 shows the EAP forwarding model via the gateway. First, the end-user function makes the EAP message and sends it to the gateway. However, the gateway cannot forward the EAP message because the link layers at each link are different. Thus the gateway uses the network layer as a transport protocol for the EAP message. The gateway will change the existing lower layer to the lower layer over the network layer and send the EAP message to the access network functions. The access network functions simply forward the packets to AM-FE, and AM-FE will process each layer for the EAP message. After processing the EAP message, the EAP message between AM-FE and TAA-FE will be delivered by an AAA protocol such as DIAMETER or RADIUS.
7.5.3 In case the mobile nodes have the PaC function

If the end-user function includes the PANA client function, the EAP message runs on the network layer from PaC to PAA. Since the end-user function including PaC can send the EAP message over the network layer, AM-FE receives the EAP message without transforming the message at the intermediate node. Acting as the enforcement point, the access network function only accepts authentication-related messages and forwards them to AM-FE.

Figure 12 – Authentication architecture for EAP over the network layer

Figure 13 illustrates the EAP forwarding model using PANA. The end-user function uses PANA as the lower layer of the EAP and sends messages over the network layer. The gateway simply forwards EAP messages and the access network functions check the type of the message. If the message is an authentication message, then the access network functions forward the message to AM-FE. AM-FE receives the EAP message and forwards it over the AAA layer to TAA-FE.
Bibliography


<http://standards.ieee.org/getieee802/>


<http://standards.ieee.org/getieee802/802.1.html>


<http://standards.ieee.org/getieee802/802.11.html>
### SERIES OF ITU-T RECOMMENDATIONS

<table>
<thead>
<tr>
<th>Series</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Series A</td>
<td>Organization of the work of ITU-T</td>
</tr>
<tr>
<td>Series D</td>
<td>General tariff principles</td>
</tr>
<tr>
<td>Series E</td>
<td>Overall network operation, telephone service, service operation and human factors</td>
</tr>
<tr>
<td>Series F</td>
<td>Non-telephone telecommunication services</td>
</tr>
<tr>
<td>Series G</td>
<td>Transmission systems and media, digital systems and networks</td>
</tr>
<tr>
<td>Series H</td>
<td>Audiovisual and multimedia systems</td>
</tr>
<tr>
<td>Series I</td>
<td>Integrated services digital network</td>
</tr>
<tr>
<td>Series J</td>
<td>Cable networks and transmission of television, sound programme and other multimedia signals</td>
</tr>
<tr>
<td>Series K</td>
<td>Protection against interference</td>
</tr>
<tr>
<td>Series L</td>
<td>Construction, installation and protection of cables and other elements of outside plant</td>
</tr>
<tr>
<td>Series M</td>
<td>Telecommunication management, including TMN and network maintenance</td>
</tr>
<tr>
<td>Series N</td>
<td>Maintenance: international sound programme and television transmission circuits</td>
</tr>
<tr>
<td>Series O</td>
<td>Specifications of measuring equipment</td>
</tr>
<tr>
<td>Series P</td>
<td>Telephone transmission quality, telephone installations, local line networks</td>
</tr>
<tr>
<td><strong>Series Q</strong></td>
<td><strong>Switching and signalling</strong></td>
</tr>
<tr>
<td>Series R</td>
<td>Telegraph transmission</td>
</tr>
<tr>
<td>Series S</td>
<td>Telegraph services terminal equipment</td>
</tr>
<tr>
<td>Series T</td>
<td>Terminals for telematic services</td>
</tr>
<tr>
<td>Series U</td>
<td>Telegraph switching</td>
</tr>
<tr>
<td>Series V</td>
<td>Data communication over the telephone network</td>
</tr>
<tr>
<td>Series X</td>
<td>Data networks, open system communications and security</td>
</tr>
<tr>
<td>Series Y</td>
<td>Global information infrastructure, Internet protocol aspects and next-generation networks</td>
</tr>
<tr>
<td>Series Z</td>
<td>Languages and general software aspects for telecommunication systems</td>
</tr>
</tbody>
</table>