International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.460.22

(01/2007)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Supplementary services for multimedia

Negotiation of security protocols to protect H.225.0 call signalling messages

ITU-T Recommendation H.460.22

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
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
Mobility interworking procedures	H.550–H.559
Mobile multimedia collaboration inter-working procedures	H.560–H.569
BROADBAND AND TRIPLE-PLAY MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619

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

ITU-T Recommendation H.460.22

Negotiation of security protocols to protect H.225.0 call signalling messages

Summary

ITU-T Recommendation H.460.22 defines a security negotiation mechanism for H.225.0 call signalling. The negotiated security mechanism between two entities is to be applied for H.225.0 call signalling messages before initiating a call establishment procedure. Detailed negotiation procedures, which provide the necessary security interoperability among H.323 systems, are specified in this Recommendation. The syntax of the security capability parameters in call signalling messages is also specified.

Source

ITU-T Recommendation H.460.22 was approved on 13 January 2007 by ITU-T Study Group 16 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. 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/.

CONTENTS

ITU-T Recommendation H.460.22

Negotiation of security protocols to protect H.225.0 call signalling messages

1 Scope

This Recommendation specifies the security negotiation mechanism for H.225.0 call signalling message exchanges. The main goals include:

1) Secure selection of the security mechanism. Otherwise, the procedure of negotiation is vulnerable to certain attacks such as malicious manipulation or bidding-down attacks. The entire RAS message shall be protected during the negotiation procedure.
2) Involved H.323 entities shall determine mutually agreed security protocols without requiring additional round trips.
3) Entities involved in the negotiation procedure shall be aware of the result of the negotiation, such as success or failure.
4) The negotiation procedure should not cause any additional burden to the involved entities.

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.225.0] ITU-T Recommendation H.225.0 (2006), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.

[ITU-T H.235.0] ITU-T Recommendation H.235.0 (2005), *H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems*.

[ITU-T H.323] ITU-T Recommendation H.323 (2006), *Packet-based multimedia communications systems*.

[ITU-T H.460.1] ITU-T Recommendation H.460.1 (2002), *Guidelines for the use of the generic extensible framework*.

[IETF RFC 4302] IETF RFC 4302 (2005), *IP Authentication Header*.

[IETF RFC 4303] IETF RFC 4303 (2005), *IP Encapsulating Security Payload (ESP)*.

[IETF RFC 4346] IETF RFC 4346 (2006), *The Transport Layer Security (TLS) Protocol Version 1.1*.

3 Definitions

This Recommendation does not define any terms.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACF Admission Confirmation

ARJ Admission Reject

ARQ Admission Request

ASN.1 Abstract Syntax Notation One

GCF Gatekeeper Confirmation

GEF Generic Extensible Framework

GRQ Gatekeeper Request

IPSec Internet Protocol Security

LCF Location Confirmation

LRJ Location Reject

LRQ Location Request

MCU Multipoint Control Unit

RAS Registration, Admission and Status

RCF Registration Confirmation

RRJ Registration Reject

RRQ Registration Request

RTP Real-time Transport Protocol

TCP Transmission Control Protocol

TLS Transport Layer Security

5 Conventions

In this Recommendation, the following conventions are used:

"Shall" indicates a mandatory requirement.

"Should" indicates a suggested but optional course of action.

"May" indicates an optional course of action rather than a recommendation that something take place.

6 Negotiation description

The protection of [ITU-T H.225.0] call signalling messages is very important for the security of an [ITU-T H.323] system. In small networks, network administrators can ensure that all H.323 entities use the same security protocol. However, in large networks, such as where endpoints are distributed in different network domains, a calling endpoint may not know in advance the security protocol supported by the called endpoint. Therefore, it is necessary for the two endpoints to negotiate the security mechanism for H.225.0 call signalling messages before initiating a call establishment procedure.

The negotiation of security protocol does not include negotiation of particular security parameters/algorithms used by the security protocol as this is outside the scope of this Recommendation. Security parameters/algorithms could be configured or negotiated out-of-band, or be part of the handshake of the security protocol.

6.1 Call establishment security

There are at least two reasons to secure a call establishment channel (i.e., H.225.0 call signalling channel). First, it is a simple way to authenticate the endpoints before accepting the call. Second, if call authorization is desired, then a secure mode of communication should be negotiated (such as TLS [IETF RFC 4346] or IPsec [IETF RFC 4302], [IETF RFC 4303] for H.323) before the exchange of call establishment messages between endpoints. Alternatively, the authorization may also be provided based upon a service-specific authentication. The constraints of a service-specific authorization policy are not considered in this Recommendation.

6.2 Negotiation of security mechanism

The generic extensible framework (GEF) feature negotiation mechanism is used during the RAS communication. Whether or not this security negotiation mechanism is supported is negotiated between the endpoint and the gatekeeper. If neither the gatekeeper nor the endpoint supports this mechanism and no other security mechanism is used, the normal H.323 procedure will be followed.

During the negotiation procedure, RAS messages can be protected by the password-based, digital signature authentication and integrity methods or by other appropriate methods.

The security negotiation procedure shall consist of the following steps:

1) The endpoint registers to the gatekeeper. The endpoint shall include the **securityProtocolNegotiation** feature in the **supportedFeatures** field in the **featureSet** structure in the RRQ message. The parameters associated with the feature indicate all the supported H.225.0 call channel security protocols. Every protocol is assigned a preference value where a smaller number signifies a higher preference.

2) The gatekeeper returns an RCF or RRJ. The gatekeeper should indicate whether the negotiation mechanism is supported or not in the RCF. If this feature is supported, the gatekeeper shall include the **securityProtocolNegotiation** feature in the **supportedFeatures** field in the **featureSet** structure. The absence of **securityProtocolNegotiation** means the gatekeeper does not support this feature. There are no parameters present in the **securityProtocolNegotiation** feature in the RCF message.

3) The endpoint initiates a call. The endpoint shall send an ARQ before SETUP by including a list of all H.225.0 call channel security protocols that are supported.

4) The next step is determined based on whether the call is routed by the gatekeeper or not:

   a) If direct call model is used, the gatekeeper shall provide all of the H.225.0 call channel security protocols supported by the called endpoint in an ACF.

   b) If the gatekeeper-routed call model is used, the gatekeeper shall provide all of the H.225.0 call channel security protocols that it supports. The gatekeeper may send an ARJ message according to security policy.

5) If the calling endpoint receives an ACF, it shall check the returned supported H.225.0 call channel security protocols in the ACF and choose a common H.225.0 call channel security protocol which the called endpoint most prefers to set up H.225.0 call signalling channel.

Figure 6-1 shows a general call flow scenario. In this scenario, it is assumed that there are at least two endpoints which belong to the same gatekeeper. These endpoints (e.g., endpoint A and endpoint B in Figure 6-1) may be H.323 terminals, MCUs, gateways etc., and are served by a single gatekeeper (named gatekeeper A). It is further assumed that H.323 endpoints communicate directly end-to-end for call establishment.

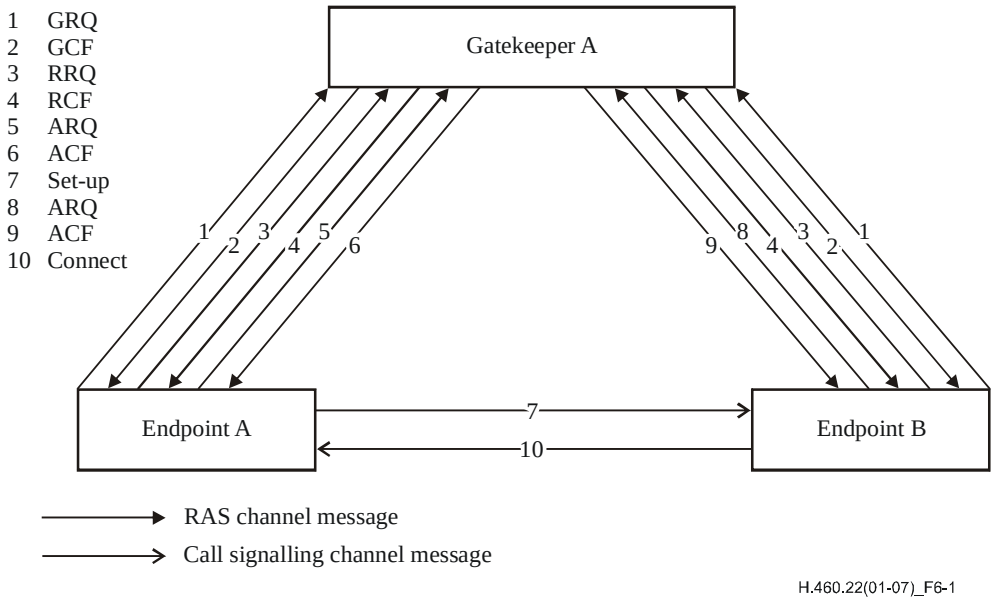

Figure 6-1 – Both endpoints are registered with the same gatekeeper – Direct call signalling

For the negotiation of a common security protocol list, the corresponding message flows of Figure 6-1 are detailed as follows:

1) Endpoints A and B send a GRQ message that includes, in the **supportedFeatures** in the **featureSet** field of the GRQ, the **securityProtocolNegotiation** feature. This feature should include all the H.225.0 call signalling channel security protocols they support.

2) The gatekeeper returns a GCF message that includes, in the **supportedFeatures** in the **featureSet** field of the GCF, the **securityProtocolNegotiation** feature. The feature negotiation procedure is optional at the GRQ/GCF stage.

3) Endpoints A and B send an RRQ that includes, in the **supportedFeatures** in the **featureSet** field, the **securityProtocolNegotiation** feature. This feature should include all of the H.225.0 call signalling channel security protocols they support.

4) The gatekeeper returns an RCF message that includes, in the **supportedFeatures** of the **featureSet** field of the RCF, the **securityProtocolNegotiation** feature. The gatekeeper shall keep the endpoint's supported security protocols for future use.

5) Before endpoint A initiates a call to endpoint B, endpoint A sends an ARQ message including the **securityProtocolNegotiation** feature with all the H.225.0 call signalling channel security protocols it supports to gatekeeper A.

6) Depending on the security policy and whether there is a common security protocol between endpoint A and endpoint B, gatekeeper A may return an ACF message including endpoint B's **securityProtocolNegotiation** feature with all of the H.225.0 call signalling channel security protocols endpoint B supports, or an ARJ to reject the call.

7) In the case where there is at least one common supported security protocol, endpoint A can establish a secure call signalling channel to endpoint B.

8) In the case where there is no common supported security protocol between endpoint A and endpoint B, gatekeeper A shall return an ARJ to endpoint A that includes **rejectReason** to stop the negotiation procedure. The rejection reason **securityDenial** is selected in **rejectReason** to denote the unsuccessful security negotiation procedure.

The above scenario with only a single gatekeeper is a special case, and a scenario with multiple gatekeepers is shown in Figure 6-2. It is assumed that there are at least two H.323 endpoints attached to different gatekeepers (e.g., endpoint A, endpoint B). It is further assumed that H.323 endpoints communicate directly end-to-end for call establishment.

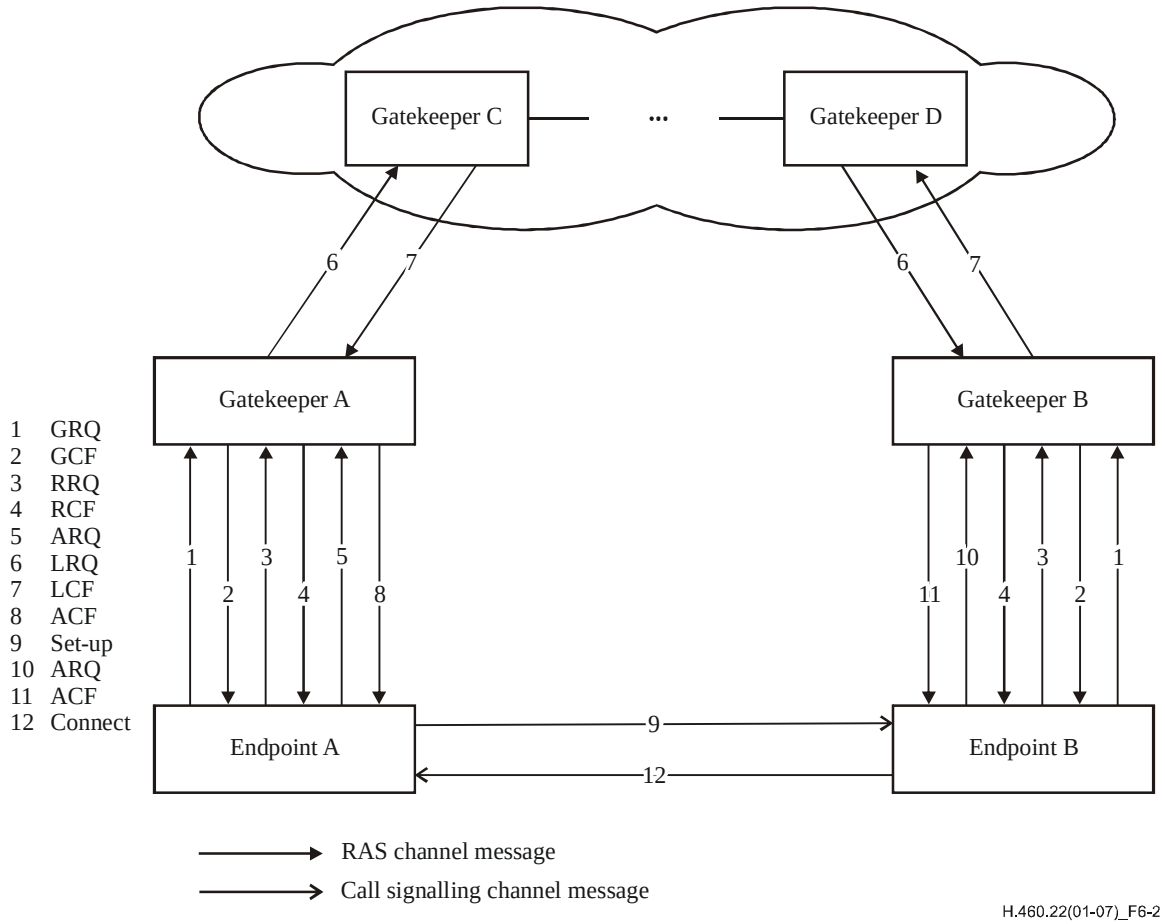

Figure 6-2 – Both endpoints are registered with different gatekeepers – Direct call signalling

The negotiation procedure described for a single gatekeeper scenario can be extended to cover multiple, chained gatekeepers. Discovery of the far-end endpoint should be accomplished according to clause 8.1.6 of [ITU-T H.323], "Optional called endpoint signalling", using **LRQ/LCF/LRJ** procedure.

The corresponding message flows are shown in Figure 6-3 and are described as follows.

1-5) The same as Steps 1-5 of the procedure for Figure 6-1.

6) After receiving the ARQ from endpoint A, gatekeeper A may send an LRQ message conveying all the security protocols supported by endpoint A to called gatekeeper B via the intermediate Gatekeepers.

7) Gatekeeper B receives the LRQ.

8) Gatekeeper B returns an LCF including all of the security protocols supported by endpoint B.

9) Gatekeeper A receives the LCF.

10) Gatekeeper A returns an ACF including all of the security protocols supported by endpoint B to endpoint A.

11) Endpoint A establishes a secure call signalling channel to endpoint B with one of the common supported security protocols. If there is no common supported security protocol between A and B, endpoint A can stop the call or proceed to set up a normal call.

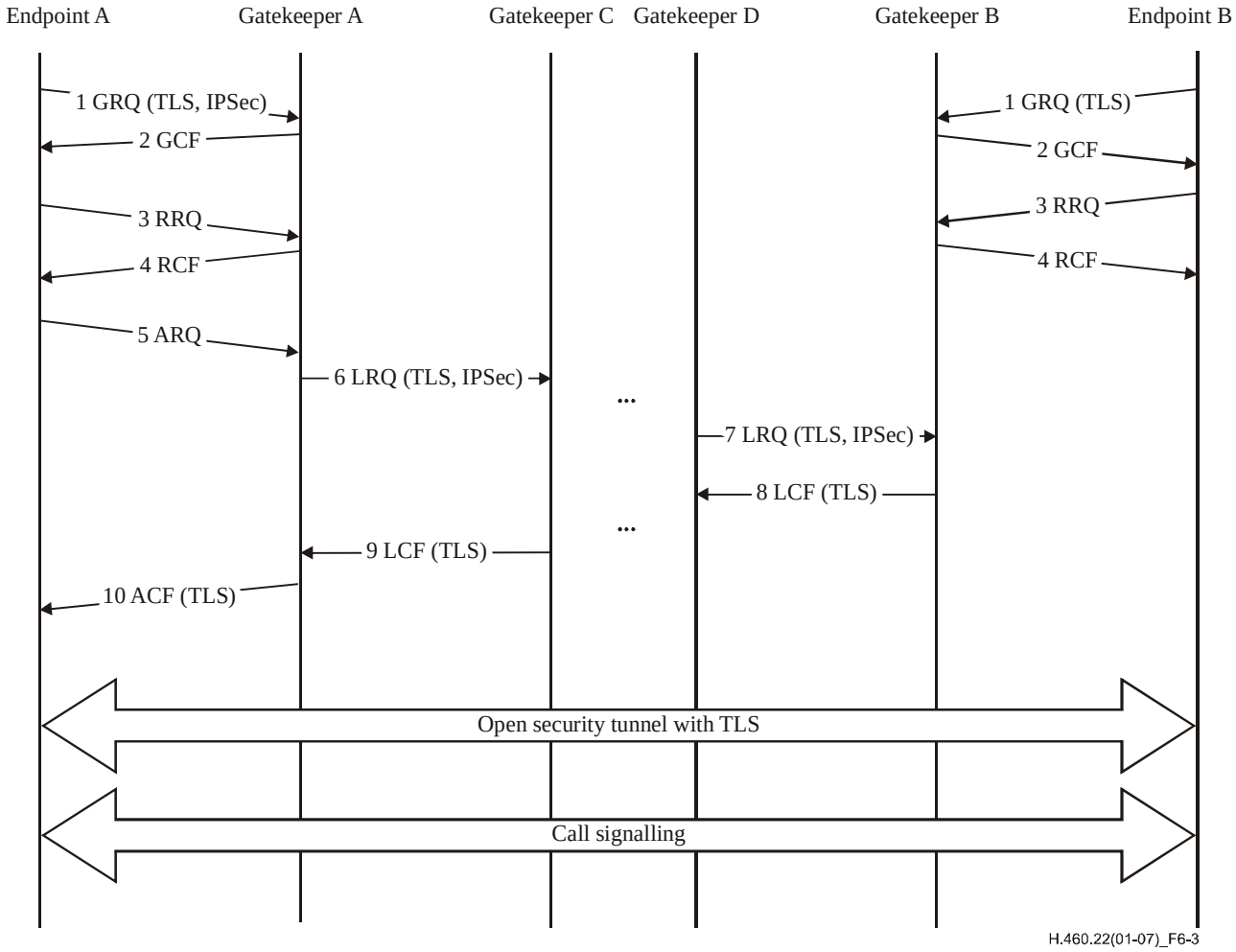

Figure 6-3 – Example negotiation signalling flow

7 Feature description securityProtocolNegotiation

H.225.0 RAS **featureSet** fields are used in this Recommendation.

The following **securityProtocolNegotiation** feature shall be present in the **supportedFeatures** field of the **featureSet** structure as shown in Table 7-1.

Table 7-1 – securityProtocolNegotiation feature

Feature name:	**securityProtocolNegotiation**
Feature description:	Shall be indicated by an entity which supports the procedure defined by this Recommendation; may be present in GRQ/GCF, RRQ/RCF, ARQ/ACF, LRQ/LCF messages.
Feature identifier type:	Standard
Feature identifier value:	22

Parameters associated with the **securityProtocolNegotiation** field are specified in the following clauses. In consideration of backward compatibility with further revisions to this Recommendation, the recipient shall simply ignore any parameters received other than those specified in this Recommendation.

7.1 tlsSecurityProtocol

The description of the **tlsSecurityProtocol** parameter is shown in Table 7-2.

Table 7-2 – tlsSecurityProtocol

Parameter name:	tlsSecurityProtocol
Parameter description:	It indicates that the TLS security protocol is supported by the entity.
Parameter identifier type:	Standard
Parameter identifier value:	1
Parameter type:	compound
Parameter cardinality:	Zero or one

It contains the two parameters shown in Tables 7-3 and 7-4 respectively.

Table 7-3 – priority

Parameter name:	priority
Parameter description:	It indicates the priority of the TLS security protocol.
Parameter identifier type:	Standard
Parameter identifier value:	1
Parameter type:	number8
Parameter cardinality:	One

Table 7-4 – connectionAddress

Parameter name:	connectionAddress
Parameter description:	It indicates the transport address used by the TLS security protocol.
Parameter identifier type:	Standard
Parameter identifier value:	2
Parameter type:	transport
Parameter cardinality:	One

7.2 ipsecSecurityProtocol

The description of the **ipsecSecurityProtocol** parameter is shown in Table 7-5.

Table 7-5 – ipsecSecurityProtocol

Parameter name:	ipsecSecurityProtocol
Parameter description:	It indicates that the IPsec security protocol is supported by the entity.
Parameter identifier type:	Standard
Parameter identifier value:	2
Parameter type:	compound
Parameter cardinality:	Zero or one

It contains the parameter shown in Table 7-6.

Table 7-6 – priority

Parameter name:	priority
Parameter description:	It indicates the priority of the IPsec security protocol.
Parameter identifier type:	Standard
Parameter identifier value:	1
Parameter type:	number8
Parameter cardinality:	One

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	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
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, 2007