International Telecommunication Union

# ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

# H.460.22

(04/2015)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Supplementary services for multimedia

# Negotiation of security protocols to protect ITU-T H.225.0 call signalling messages

Recommendation ITU-T 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 |
| Telepresence | H.420–H.429 |
| **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, TRIPLE-PLAY AND ADVANCED MULTIMEDIA SERVICES | |
| Broadband multimedia services over VDSL | H.610–H.619 |
| Advanced multimedia services and applications | H.620–H.629 |
| Ubiquitous sensor network applications and Internet of Things | 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 SERVICES AND APPLICATIONS | |
| 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 |

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

## Recommendation ITU-T H.460.22

# Negotiation of security protocols to protect ITU-T H.225.0 call signalling messages

### Summary

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

This revision includes procedural clarifications and introduces support for ITU-T H.460.18 and ITU-T H.460.19 NAT traversal and negotiating datagram transport layer security (DTLS) for ITU-T H.323 Annex E over UDP transport.

### History

| Edition | Recommendation | Approval | Study Group | Unique ID* |
|---|---|---|---|---|
| 1.0 | ITU-T H.460.22 | 2007-01-13 | 16 | 11.1002/1000/9041 |
| 1.1 | ITU-T H.460.22 (2007) Cor. 1 | 2008-06-13 | 16 | 11.1002/1000/9489 |
| 2.0 | ITU-T H.460.22 | 2015-04-29 | 16 | 11.1002/1000/12456 |

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

## FOREWORD

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

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

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

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

## NOTE

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

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

## INTELLECTUAL PROPERTY RIGHTS

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

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

## Table of Contents

# Recommendation ITU-T H.460.22

# Negotiation of security protocols to protect ITU-T H.225.0 call signalling messages

## 1 Scope

This Recommendation specifies the security negotiation mechanism for ITU-T H.225.0 call signalling message exchanges. The main goals include the following.

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 registration, admission and status (RAS) message shall be protected during the negotiation procedure.

2) Involved [ITU-T 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] Recommendation ITU-T H.225.0 (2009), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.

[ITU-T H.235.6] Recommendation ITU-T H.235.6 (2014), *H.323 security: Encryption profile with native ITU-T H.235/H.245 key management*.

[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.323] Recommendation ITU-T H.323 (2009), *Packet-based multimedia communications systems*.

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

[ITU-T H.460.17] Recommendation ITU-T H.460.17 (2005), *Using H.225.0 call signalling connection as transport for H.323 RAS messages*.

[ITU-T H.460.18] Recommendation ITU-T H.460.18 (2013), *Traversal of ITU-T H.323 signalling across network address translators and firewalls*.

[IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

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

## 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 |
| DTLS | Datagram Transport Layer Security |
| FW | Firewall |
| 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 |
| MiTM | Man in The Middle |
| NAT | Network Address Translator |
| RAS | Registration, Admission and Status |
| RCF | Registration Confirmation |
| RRJ | Registration Reject |
| RRQ | Registration Request |
| SCI | Service Control Indication |
| 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 important for the security of ITU-T H.323 systems. In small networks, network administrators can ensure that all ITU-T 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 ITU-T H.225.0 call signalling messages before initiating a call establishment procedure.

The negotiation of actual security parameters/algorithms is outside the scope of this Recommendation.

## 6.1 Call establishment security

There are a number of important reasons to secure the call signalling channel (i.e., ITU-T H.225.0). When using [ITU-T H.235.6] or [ITU-T H.235.8] to encrypt the media packets, the keys are exchanged in the signalling channel. These keys are sent either in the clear and require a secure signalling channel or are susceptible to man in the middle (MiTM) attacks and should be protected by a secure call signalling channel. It also provides a very simple way to authenticate the endpoints to each other in direct call signalling mode or for each hop of the call in gatekeeper routed mode.

## 6.2 Negotiation of security mechanism

The generic extensible framework (GEF) feature negotiation mechanism [ITU-T H.460.1] 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 [ITU-T H.323] procedure will be followed.

The security negotiation procedure shall consist of the following steps.

1) The endpoint, where enabled, discovers the gatekeeper. The endpoint shall advertise the **securityProtocolNegotiation** feature as a **supportedFeature** in the **featureSet** field of the gatekeeper request (GRQ). All parameters of the **securityProtocolNegotiation** feature shall be omitted. Where the gatekeeper supports this feature, it shall advertise as a **supportedFeature** with all parameters omitted in the reply GRQ. The absence of s**ecurityProtocolNegotiation** feature indicates the gatekeeper does not support this feature.

2) Where the endpoint has discovered support for this feature or is registering without discovery, the endpoint shall include the **securityProtocolNegotiation** feature as a **supportedFeature** in the **featureSet** field in the registration request (RRQ) message. The parameters associated with the feature shall indicate all the security protocols supported by the endpoint. Every protocol is assigned a preference value, where a smaller number signifies a higher preference. The gatekeeper stores this information for call establishment purposes. Lightweight RRQs shall only include the **securityProtocolNegotiation** feature advertisement and omit all parameters.

3) The gatekeeper returns a registration confirmation (RCF) or registration reject (RRJ). The gatekeeper shall indicate whether the negotiation mechanism is supported in the RCF. If this feature is supported, the gatekeeper shall include the **securityProtocolNegotiation** feature as a **supportedFeature** in the **featureSet** field. The absence of **securityProtocolNegotiation** shall indicate that the gatekeeper does not support this feature. There are no parameters present in the **securityProtocolNegotiation** feature in the RCF message.

4) The endpoint initiates a call. The endpoint shall send an ARQ to the gatekeeper including a **securityProtocolNegotiation** feature as a **supportedFeature** in the **featureSet** field of the admission request (ARQ). All parameters shall be omitted.

5) The next step is determined based on whether the call is routed by the gatekeeper.

   a) If direct call model is used, the gatekeeper shall send an ARQ containing the highest priority matching security protocol supported by both endpoints and shall include the stored connnectionAddress of the called endpoint where applicable. The **priority** field shall be omitted.

b) If the gatekeeper-routed call model is used, the gatekeeper shall send an ARQ containing the highest priority matching security protocols that the calling endpoint and gatekeeper support and shall include the gatekeeper's **connectionAddress** where applicable. The **priority** field shall be omitted. The gatekeeper may send an admission reject (ARJ) message if there is no matching security protocol.

6) If the calling endpoint receives an admission confirmation (ACF), it shall check the returned supported security protocol in the ACF and use the security protocol to set up an ITU-T 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 ITU-T H.323 terminals, multipoint control units (MCUs), gateways, etc., and are served by a single gatekeeper (named gatekeeper A). It is further assumed that ITU-T H.323 endpoints communicate directly end-to-end for call establishment.

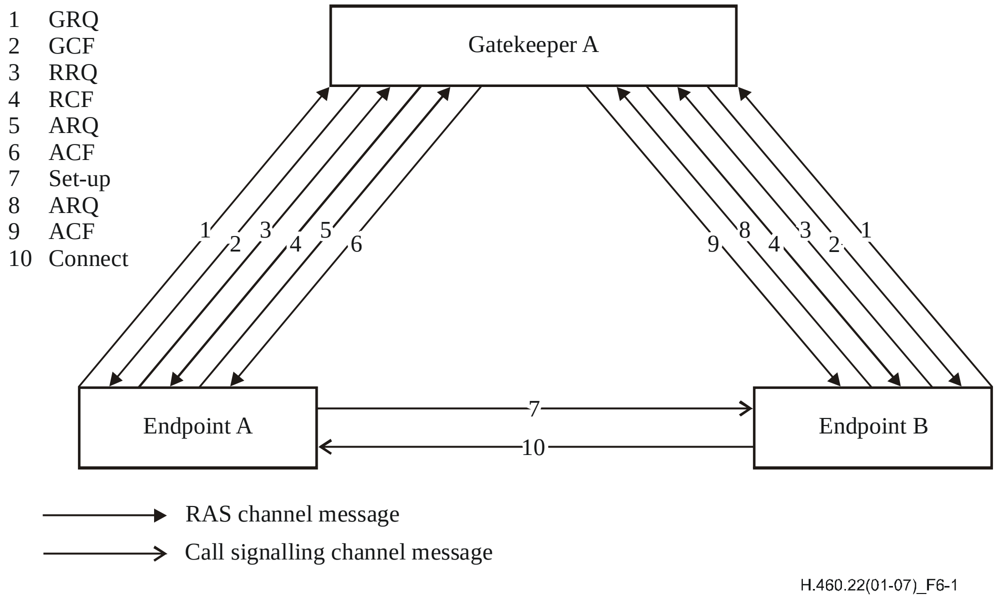

**Figure 6-1 – Both endpoints are registered with the same gatekeeper – Direct call signalling**

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.

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 security protocols including priority and connectionAddress (where applicable) 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 to gatekeeper A.

6) Depending on the security policy and whether the call signalling is gatekeeper routed, gatekeeper A in direct mode, may return an ACF message including endpoint B's

**securityProtocolNegotiation** feature with the highest priority matching security protocol between endpoint A and endpoint B, In routed mode, it may return the highest matching security protocol between endpoint A and the gatekeeper or due to security policy may return an ARJ to reject the call.

7) If there is at least one common supported security protocol, in direct mode, endpoint A establishes a secure call signalling channel to endpoint B. In routed mode, endpoint A establishes a secure call signalling channel with the gatekeeper and the gatekeeper in turn establishes a secure call signalling channel to endpoint B.

8) If there is no common supported security protocol between endpoint A and the gatekeeper and/or endpoint B, and where gatekeeper security policy permits, endpoint A may proceed to set up a normal call.

A scenario with multiple gatekeepers is shown in Figure 6-2. It is assumed that there are at least two ITU-T H.323 endpoints attached to different gatekeepers (e.g., endpoint A, endpoint B). It is further assumed that ITU-T H.323 endpoints communicate directly end-to-end for call establishment.

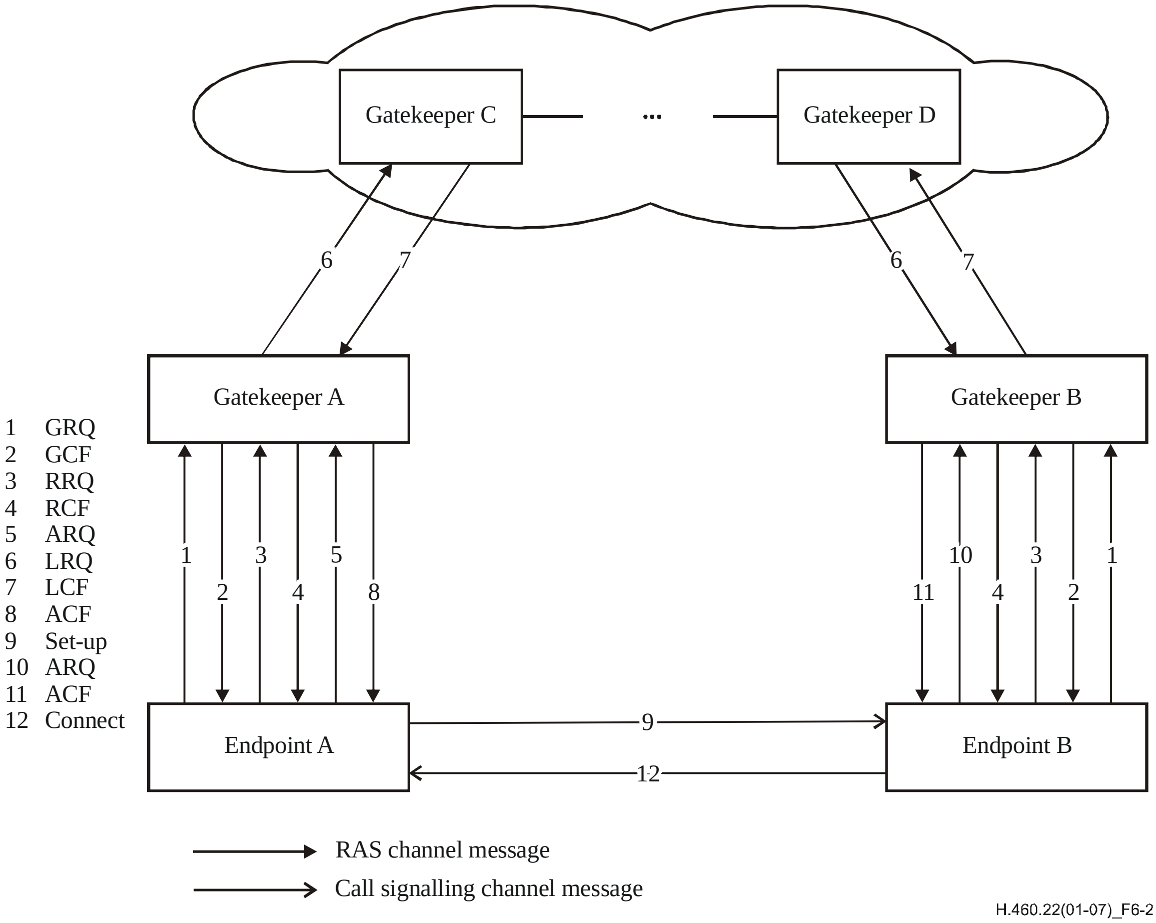

**Figure 6-2 – Both endpoints are registered with different gatekeepers – Direct call signalling**

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 the location request/location confirmation/location reject (**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 the highest priority matching security protocol between endpoint A and endpoint B and/or gatekeeper B depending on the call signalling routing mode. Where signalling is gatekeeper routed, the protocol returned shall be the highest matching of gatekeeper B. Where signalling is direct (not gatekeeper routed) the protocol shall be the highest matching of endpoint B. The appropriate **connectionAddress** parameter (where applicable) shall be included and the **priority** parameter shall be omitted.

9) Gatekeeper A receives the LCF.

10) Gatekeeper A returns an ACF including the security protocol information received in the LCF.

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

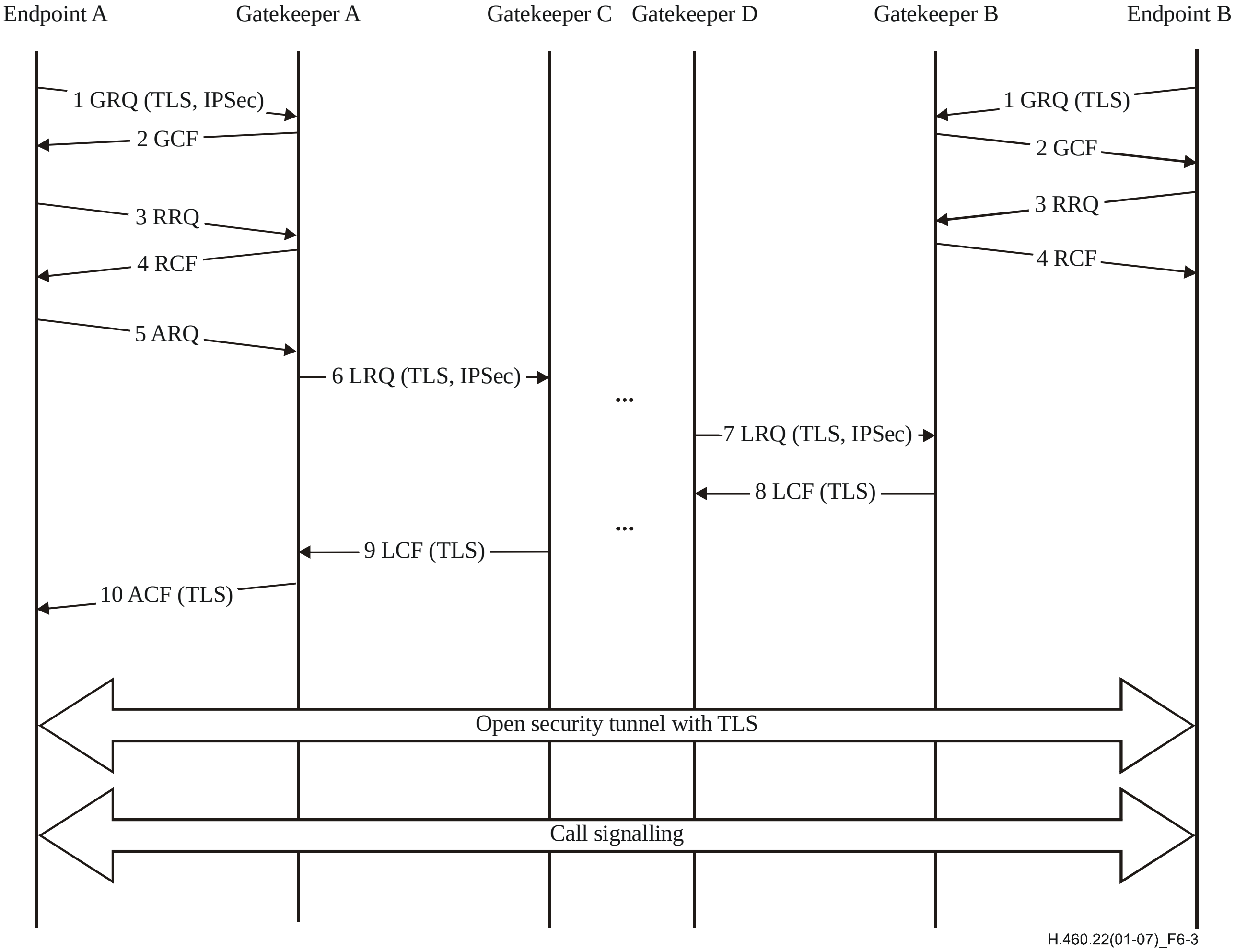

**Figure 6-3 – Example negotiation signalling flow**

## 7 Feature description securityProtocolNegotiation

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

The following **securityProtocolNegotiation** feature shall be presented as a **supportedFeature** in the **featureSet** field 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

This Recommendation may be used to offer and utilize transport layer security (TLS) [IETF RFC 5246] to secure ITU-T H.225.0 call signalling.

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 |

The **tlsSecurityProtocol** parameter shall contain 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

This Recommendation may be used to offer and utilize internet protocol security (IPsec) to secure [ITU-T H.225.0] call signalling messages.

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 protocol is supported by the entity. |
| Parameter identifier type: | Standard |
| Parameter identifier value: | 2 |
| Parameter type: | compound |
| Parameter cardinality: | Zero or one |

The **ipsecSecurityProtocol** parameter shall contain the parameter shown in Table 7-6.

**Table 7-6 – priority**

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

## 7.3 dtlsSecurityProtocol

This Recommendation may be used to offer and utilize datagram transport layer security (DTLS) [IETF RFC 6347] to secure [ITU-T H.225.0] call signalling messages using the [ITU-T H.323] Annex E transport as defined in clause E.2 of [ITU-T H.323].

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

**Table 7-7 – dtlsSecurityProtocol**

| | |
|---|---|
| Parameter name: | dtlsSecurityProtocol |
| Parameter description: | It indicates that the DTLS security protocol is supported by the entity. |
| Parameter identifier type: | Standard |
| Parameter identifier value: | 3 |
| Parameter type: | compound |
| Parameter cardinality: | Zero or one |

The **dtlsSecurityProtocol** parameter shall contain the two parameters shown in Table 7-8 and 7-9 respectively.

**Table 7-8 – priority**

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

**Table 7-9 – connectionAddress**

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

## 8 NAT traversal considerations

When using this feature with [ITU-T H.460.18], consideration needs to be given to inbound calling to an endpoint behind a network address translator/firewall (NAT/FW). In this scenario, direct call signalling connection from outside of the NAT/FW to inside is impossible and an RAS pinhole needs to be maintained to allow the endpoint behind the NAT/FW to be notified of an inbound call. The call signalling connection needs to be establish from behind the NAT/FW to the gatekeeper. All call signalling is required to be gatekeeper routed.

Clause 10 of [ITU-T H.460.18] describes the method by which an endpoint behind a NAT/FW is notified of an inbound call by sending an RAS service control indication (RAS SCI) message with a **genericData** field containing the **IncomingCallIndication** parameter. This notifies the endpoint of the call signalling address to establish an outbound transmission control protocol (TCP) connection.

When using this Recommendation in conjunction with [ITU-T H.460.18], the RAS SCI message specified in clause 10 of [ITU-T H.460.18] shall also contain this feature in the **genericData** field. It shall also contain the security protocol and the **connectionAddress** (where applicable) of the gatekeeper to establish the secure connection. The priority field shall be omitted.

This Recommendation is incompatible with [ITU-T H.460.17] and should not be advertised when registering to a gatekeeper using [ITU-T H.460.17].

## 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