INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.235

Annex F

(03/2002)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Systems aspects

Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals

Annex F: Hybrid security profile

ITU-T Recommendation H.235 – Annex F

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.399
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

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

ITU-T Recommendation H.235

Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals

Annex F

Hybrid security profile

Summary

The purpose of this annex is to describe an efficient and scalable, PKI-based hybrid security profile for Version 2 of H.235. The hybrid security profile contained herein takes advantage of the security profiles in H.235 Annex D and in H.235 Annex E by deploying digital signatures from H.235 Annex E and deploying the baseline security profile from H.235 Annex D.

Source

Annex F to ITU-T Recommendation H.235 was prepared by ITU-T Study Group 16 (2001-2004) and approved under the WTSA Resolution 1 procedure on 29 March 2002.

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.

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, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

ITU-T Recommendation H.235

Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals

Annex F

Hybrid security profile

F.1 Overview

This annex describes an efficient and scalable, PKI-based hybrid security profile deploying digital signatures from H.235 Annex E and deploying the baseline security profile from H.235 Annex D. This annex is suggested as an option. H.323 security entities (terminals, gatekeepers, gateways, MCUs, etc.) may implement this hybrid security profile for improved security or whenever required.

The notion of "hybrid" in this text shall mean that security procedures from the signature profile in H.235 Annex E are actually applied in a lightweight sense and the digital signatures still conform to the RSA procedures. However, digital signatures are deployed only where absolutely necessary while highly efficient symmetric security techniques from the baseline security profile in H.235 Annex D are used otherwise.

The hybrid security profile is applicable for scaleable "global" IP telephony. This security profile overcomes the limitations of the simple, baseline security profile of H.235 Annex D when strictly applying it. Furthermore, this security profile overcomes certain drawbacks of H.235 Annex E such as the need for higher bandwidth and increased performance needs for processing when strictly applying it. For example, the hybrid security profile does not depend on the (static) administration of mutual shared secrets of the hops in different domains. Thus, users can much more easily choose their VoIP provider. Thus, this security profile supports a certain kind of user mobility as well. It applies asymmetric cryptography with signatures and certificates only where necessary and otherwise uses simpler and more efficient symmetric techniques. It provides tunnelling of H.245 messages for H.245 message integrity and also implements some provisions for non-repudiation of messages.

The hybrid security profile mandates the GK-routed model and is based upon the H.245 tunnelling techniques. Support for non GK-routed models is for further study.

The features provided by this profile include:

For RAS, H.225.0 and H.245 messages:

- User authentication to a desired entity irrespective of the number of application level hops[1] that the message traverses.
- Integrity of all or critical portions (fields) of messages arriving at an entity irrespective of the number of application-level hops that the message traverses. Integrity of the message itself using a strongly generated random number is also optional.

[1] Hop is understood here in the sense of a trusted H.235 network element (e.g. GK, GW, MCU, proxy, or firewall). Thus, application level hop-by-hop security when used with symmetric techniques does not provide true end-to-end security between terminals.

- Application-level hop-by-hop message authentication, integrity and (some) non-repudiation provide these security services for the entire message.
- Using the available public-key infrastructure, users can choose their service provider. Key-management for session key distribution is well integrated in the hybrid security profile.

Suitable provision of the above-described security services thwarts several types of attacks, including:

- *Man-in-the-middle attacks*: Application-level hop-by-hop message authentication and integrity prevents against such attacks when the man-in-the-middle is in an application-level hop, say, a hostile router.
- *Replay attacks*: Use of timestamps and sequence numbers prevent such attacks.
- *Spoofing*: User authentication prevents such attacks.
- *Connection hijacking*: Use of authentication/integrity for each signalling message prevents such attacks.

F.2 Normative 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 bellow. A list of the currently valid ITU-T Recommendations is regularly published.

– ITU-T Recommendation H.225.0, Version 4 (2000), *Call signalling protocols and media stream packetization for packe- based multimedia communication systems*.

– ITU-T Recommendation H.323, Version 4 (2000), *Packet-based multimedia communications systems*.

– Recommendation H.235, Version 2 (2000), *Security and encryption for H-series (H.323 and other H.245-Based) multimedia terminals*.

– ITU-T Recommendation H.245, Version 8 (2001), *Control protocol for multimedia communication*.

– IETF RFC 2459 (1999), *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*.

F.3 Acronyms

This annex defines the following acronyms:

GCF Gatekeeper Confirm

GK Gatekeeper

GRQ Gatekeeper Request

ICV Integrity Check Value

LRQ Location Request

OID Object Identifier

RAS Registration, Admission and Status

RCF Registration Confirm

RRQ Registration Request

RSA Rivest, Shamir and Adleman encryption algorithm

SHA Secure Hash Algorithm

URQ Unregistration request

F.4 Specification conventions

The hybrid security profile uses terms and definitions from Annexes D and E of H.235.

While the message integrity service always provides message authentication, the reverse is not always true. For the authentication-only mode, the integrity assured only spans a certain subset of message fields. This applies to integrity services realized by asymmetric means (e.g. digital signatures). Thus, in practice, combined authentication and integrity service exploit the same key material without introducing a security weakness.

This security profile is applicable in environments with potentially many terminals, where static password/symmetric key assignment is not feasible, e.g. in large-scale or global-scale scenarios. Instead, this security profile assumes availability of a public-key infrastructure with assigned certificates and private/public-keys, directories, etc. In addition, this security profile deploys symmetric crypto techniques where applicable.

This security profile introduces the terms "first" message and "last" message sent. Security protection of the first message (and probably also for the last message) is different from security protection of the remaining other messages.

The "first message" sent is understood as a message that flows between two H.323 entities and establishes a security context. It makes symmetric key material available to both entities and, for example, marks the beginning of a call. For H.225.0 RAS, the first message is the RRQ and the related response message. For H.225.0 call signalling using fast start, the first message is SETUP and CONNECT.

The "last message" terminates the established security context. The established key material shall be destroyed. For H.225.0 RAS, the last message is the URQ and related response message, while for H.225.0 call signalling the last message is RELEASE-COMPLETE.

This security profile assumes the GK-routed call model, where the fast connect call signalling method is applied. H.245 call control messages are securely tunnelled in H.225.0 call signalling messages and inherit thereby the H.225.0 security protection scheme.

The signature security profile allows to securely tunnel H.245 call control PDUs within H.225.0 facility messages. The H.245 key update and synchronization mechanisms require tunnelling for key-update FACILITY message to be signalled and is useful, for example, for very long duration calls.

The light gray shaded area in Table F.1 represents the security mechanisms that are used by the hybrid security profile.

NOTE – RSA certificates with MD5 hashing are not part of this security profile.

The voice encryption security profile of H.235 Annex D (see D.7) could be optionally used in conjunction with the hybrid security profile. Its use is negotiated as part of the call set-up signalling.

Table F.1/H.235 – Overview of the hybrid security profile

Security services	Call functions			
	RAS	**H.225.0**	**H.245 (Note 3)**	**RTP**
Authentication	RSA digital signature (SHA1)	RSA digital signature (SHA1)	RSA digital signature (SHA1)	
	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	
Non-repudiation	(possible only on first message)	(possible only on first message)		
Integrity	RSA digital signature (SHA1)	RSA digital signature (SHA1)	RSA digital signature (SHA1)	
	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	
Confidentiality				
Access control				
Key management	certificate allocation	certificate allocation		
	authenticated Diffie-Hellman key-exchange	authenticated Diffie-Hellman key-exchange		

NOTE 1 – The hybrid security profile has to be also supported by other H.235 entities (e.g. gatekeepers, gateways and H.235 proxies).

NOTE 2 – Available key usage bits in the certificate could also determine the security service provided by a terminal (e.g. non-repudiation asserted).

NOTE 3 – Tunnelled H.245 or embedded H.245 inside H.225.0 fast connect.

For authentication, the user should use a public/private key signature scheme. Such a scheme usually provides for better integrity.

This Recommendation does not describe procedures for registration, certification and certificate allocation from a trust center and private/public key assignment, directory services, specific CA parameters, certificate revocation, key pair update/recovery and other certificate operational or management procedures such as certificate or public/private key and certificate delivery and installation in terminals. Such procedures may happen by means that are not part of this annex.

The communication entities involved are able to implicitly determine usage of either the H.235 Annex D baseline security profiles, H.235 Annex E signature profile, or this hybrid security profile by evaluating the signaled security object identifiers in the messages (**tokenOID**, and **algorithmOID**; see also E.8).

F.5 H.323 requirements

H.323 entities that implement this hybrid security profile are assumed to support the following H.323 features:

- Fast connect;
- H.245 tunnelling; and
- GK-routed model.

F.6 Authentication and integrity

This annex uses the following terms for provisioning the security services.

- **Authentication and integrity**: This is a combined security service that supports message integrity in conjunction with user authentication. The user authenticates when either correctly digitally signing some piece of data with the private key or when correctly applying a related, shared secret. In addition to that, the message is protected against tampering. Both security services are provided by the same security mechanism. Combined authentication and integrity is possible only on a hop-to-hop basis.

NOTE – When digital signatures are applied, a non-repudiation security service may be supported. This also depends on the settings of the key usage bits of the signing key in the certificate (see also RFC 2459).

We describe the following procedures for use in this profile.

Procedure IV is based on digital signatures using a private/public key pair and deploying symmetric crypto techniques for providing authentication and integrity of RAS, Q.931 and H.245 messages. Terminals may use this method if efficient, scalable security is required.

Depending on the security policy, authentication may be unilateral or mutual (i.e. applying the authentication/integrity in the reverse direction as well, thereby providing higher security). The preferred security mode is to have mutual authentication.

Gatekeepers detecting failed authentication and/or failed integrity validation in a RAS/call signalling message received from a terminal/peer gatekeeper will respond with a corresponding reject message indicating security failure. This is done by setting the reject reason to **securityDenial** or other appropriate security error code according to H.235 clause B.2. As part of the returned response, the sender may provide a list of acceptable certificates in separate tokens, in order to facilitate selection of an appropriate one by the recipient.

There is implicit H.235 signalling for indicating use of procedure IV and the applied security mechanism based upon the value of the object identifiers (see also F.12) and the message fields filled-in. In this text, object identifiers are referenced symbolically through letters (e.g. "A").

This profile does not use the H.235 ICV fields. Rather, cryptographic integrity check values are put into the **signature** field of the **token** in the **cryptoSignedToken** when referring to Annex E, or the integrity check values are put in the hash fields of the **CryptoToken** when referring to Annex D.

F.7 Procedure IV

The following procedures shall be adhered to if procedure IV is employed for hop-by-hop security. This procedure unites Procedure I of Annex D (see D.6.3.2) and Procedure II of Annex E (see E.5).

For the first message including corresponding response sent in each direction, Annex E procedure II (hop-by-hop authentication and integrity, see E.5) shall be used with the following settings:

- OID "A1" instead of OID "A" and OID "S1" instead of OID "S". Use of these OIDs allows identifying the hybrid security profile.
- **algorithmOID** in **tokenOID** shall be set to "W" indicating use of RSA-SHA1 signature.
- **signature** shall contain an ASN.1 encoded RSA signature (see E.10/H.235).
- **certificate** should contain the sender's user certificate if not available otherwise to the receiver.

In a single administrative domain scenario the first message/response is defined as initial the H.225.0 RAS message/response; this is usually either GRQ/GCF or RRQ/RCF. In a multi-administrative domain scenario, the first message/response within each domain is defined as above; the first message between the domains is defined as SETUP.

Sender and recipient exchange and compute an authenticated Diffie-Hellman secret bit string. Table D.4/H.235 provides an example of Diffie-Hellman group parameters and recommends taking the 1024-bit prime whenever possible, for security reasons. The Diffie-Hellman secret shall be computed for each leg, regardless of whether the voice encryption profile is deployed or not.

From the common bit string that both parties compute, both parties derive a 160-bit secret by taking the least significant 160 bits. The resulting 160-bit secret acts as the password/shared secret that is used in Annex D.

In a scenario with gatekeepers in distinct administrative domains, sender and receiver shall use two tokens in each direction for H.225.0 call signalling:

- One **ClearToken** inside **CryptoToken**, which is used to compute the media key that is shared among the terminals (see D.7.1). This is only necessary if voice encryption is to be deployed.
- A separate **ClearToken** is used to compute a link key that is shared among the sender and receiver entities for protection of the signalling link. This link key replaces the shared password among the gatekeepers in Annex D. The **tokenOID** of that **ClearToken** shall be set to "Q", indicating use of Diffie-Hellman and hybrid security profile. Computation of the link key proceeds in the same manner as computation of the media key (see D.7.1).

NOTE – For direct-routed environments, sender/receiver entities and terminals correspond. For GK-routed environments, the link key is shared hop-by-hop between each pair of peer gatekeepers, while the media key is shared on an end-to-end basis.

In GK-routed environments, the GK shall forward the received Diffie-Hellman token from the endpoint to the next hop.

For all but the very first message/response sent in each direction, Annex D procedure I (see D.6.3.2) shall be used. This applies also in a scenario where multiple gatekeepers are located within an administrative domain. In this case there is no need for asymmetric key management; instead, H.235 Annex D is sufficient.

This annex may be used with H.235 Version 1 systems when taking care of restricted use of senders ID and generalID, as described in H.235 clause E.17.

F.8 Security association for concurrent calls

An optimization is provided for the case that a fixed pair of entities would process several independent calls in parallel using a single call signalling channel. Instead of establishing several link keys with Diffie-Hellman for each call, a security association is defined which spans multiple concurrent calls.

More precisely, the security association spans all calls between a fixed pair of entities as long as the call signalling channel is alive. Entities use the **multipleCalls** flag within Setup to indicate the capability of signalling multiple calls over a single call signalling connection, (see 7.3/H.323).

If the single call signalling connection is used, then only one common link key needs to be established, see Figure F.1.

On the other hand, if the **multipleCalls** flag within SETUP is not set, then a link key shall be individually computed anew for each call.

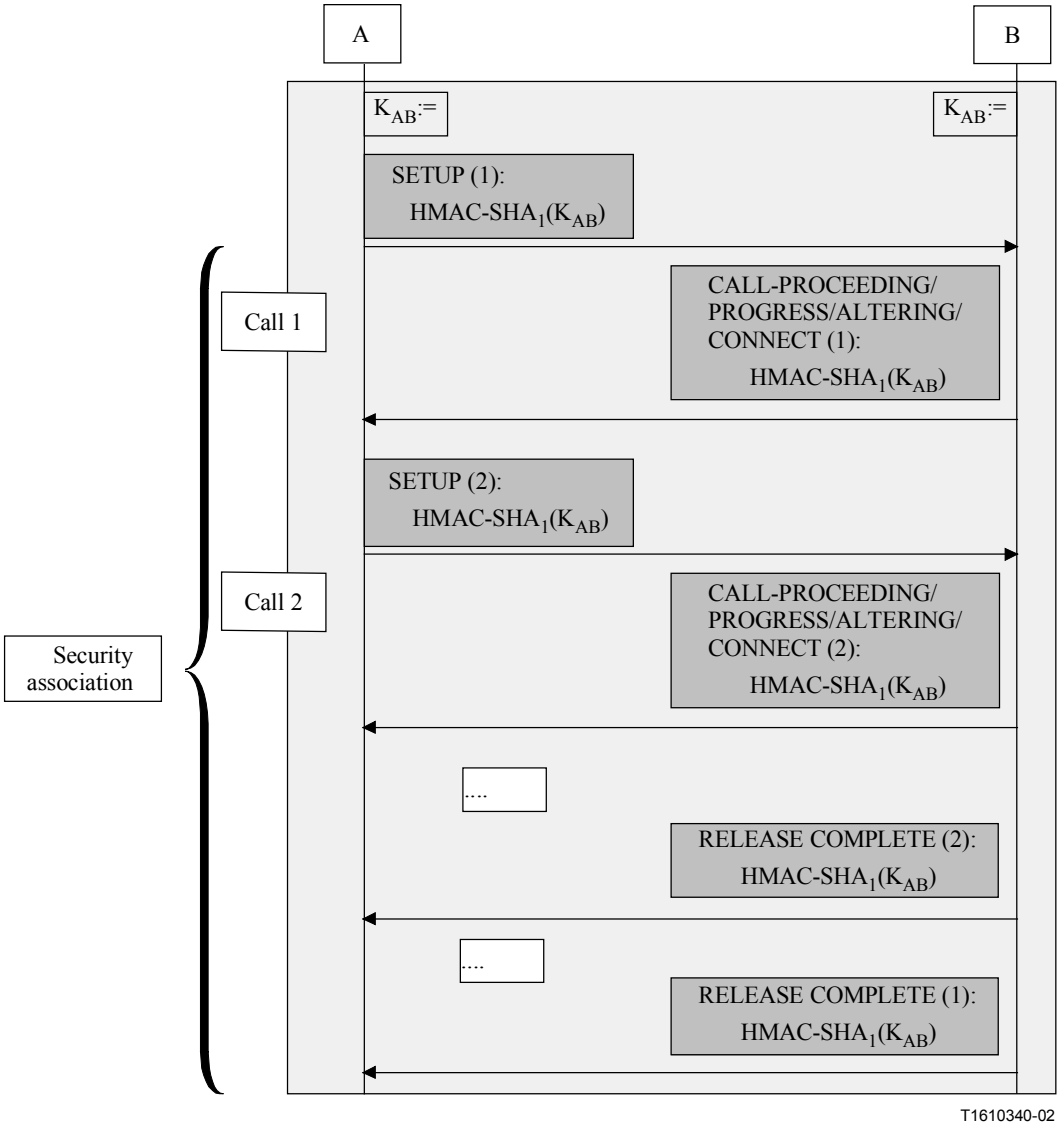


Figure F.1/H.235 – Security association for concurrent calls

F.9 Key update

An optional key update procedure allows either communication entity (GK or terminal) to refresh the currently-used session key with a new one. Such a key update should be initiated by whichever entity feels a need for it. A key update may be motivated by a compromised session key, the perception that the session key has or will become insecure, or other security policy criteria. These aspects are all outside the scope of this Recommendation.

The initiator invokes the key update using the FACILITY message. The FACILITY message for key update conveys a new Diffie-Hellman token, an optional digital certificate, and a digital signature of the initiator. Upon reception of the FACILITY message, the recipient replies with a similar FACILITY message conveying his Diffie-Hellman token, an optional digital certificate, and a digital signature of the recipient. Upon completion of the key update procedure, initiator and responder shall use the computed new link key.

- **tokenOID** of the **ClearToken** within FACILITY shall be set to "Q" indicating use of Diffie-Hellman and hybrid security profile. Computation of the link key proceeds in the same manner as computation of the media session key (see D.7.1).

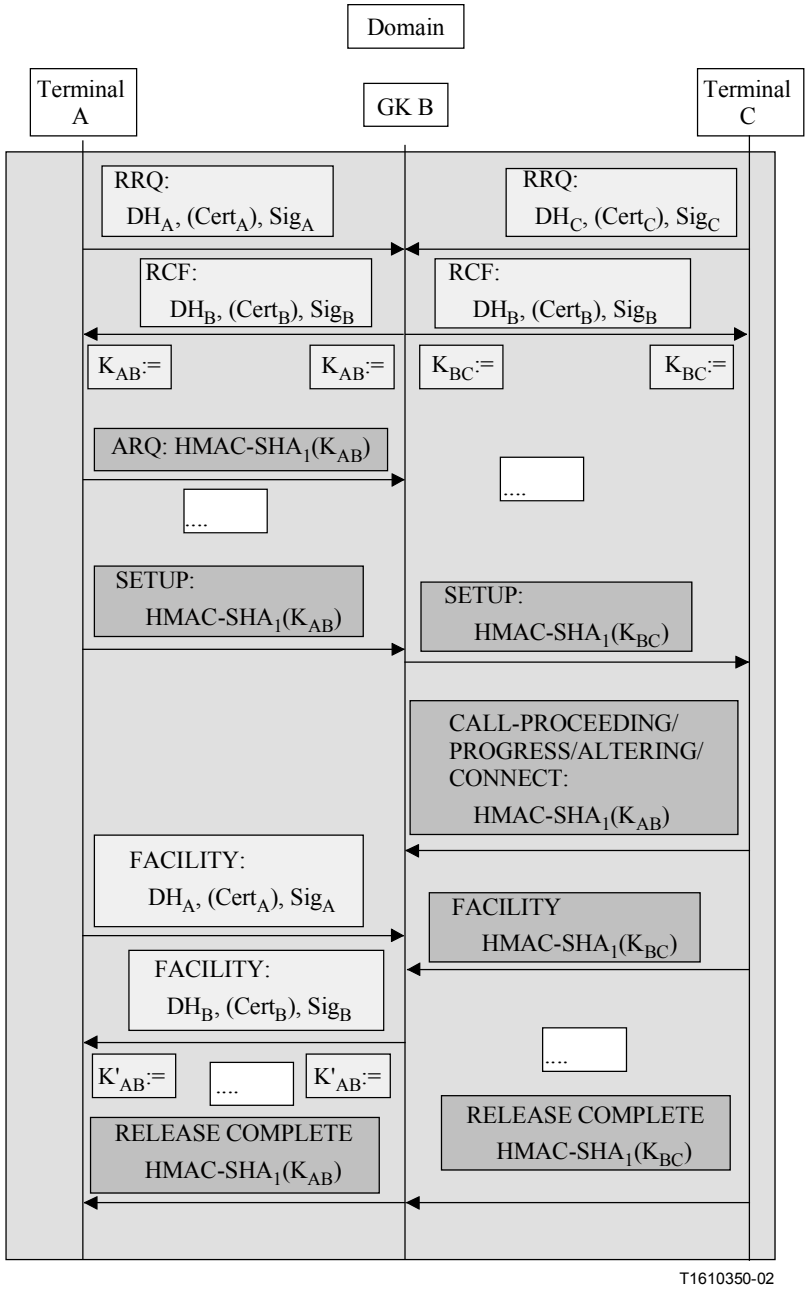
The FACILITY message for key update purposes shall be protected according to H.235 Annex E Procedure II. Any other FACILITY message without conveyed Diffie-Hellman token shall not be deployed for key update purposes and shall be protected according to H.235 Annex D Procedure I.

F.10 Illustration examples

The flow diagrams in Figures F.2 and F.3 illustrate usage of Annex F in a basic message flow. Note that the diagrams do not show the complete message flow and that several messages are omitted for simplicity. Messages highlighted in light gray relate to the signature profile H.235 Annex E, while dark gray messages relate to the baseline profile H.235 Annex D. The figures emphasize the (most important) security parts of each message (H.235 CryptoTokens, Tokens) while omitting details.

The flow diagram in Figure F.2 illustrates the basic message flow in a scenario with one gatekeeper within a single administrative domain. Assuming that the gatekeeper certificate is known to all the terminals involved and that the terminals know the gatekeeper certificate likewise, there is no need to transmit the certificates in-band during the registration procedure.

NOTE 1 – Figures F.2 and F.3 below cover also the fast start procedure when the call signalling messages SETUP and CALL PROCEEDING/PROGRESS/ALERTING/CONNECT include the faststart token (see 8.1.7/H.323). Otherwise, non-faststart mode is assumed according to 7.3.1/H.323. Figure F.2 shows also the key update procedure between Terminal A and Gatekeeper B using FACILITY.



Cert	User certificate	K, K'	symmetric link key
DH_A	Diffie-Hellman Token g^a mod p	Sig	digital signature
DH_B	Diffie-Hellman Token g^b mod p		
EP	Endpoint (Terminal)		
GK	Gatekeeper		

Figure F.2/H.235 – Flow diagram in a single administrative domain

Figure F.3 shows an example message flow in a scenario with different administrative domains. While the hybrid security profile is applied within each domain between terminal and gatekeeper as illustrated in Figure F.2, the hybrid security profile may be applied also between both domains during the call establishment phase.

NOTE 2 – Figure F.3 omits any communication among border elements (BE) and any communication between GK-to-BE. Figure F.3 also shows the key update procedure between both domains using FACILITY.

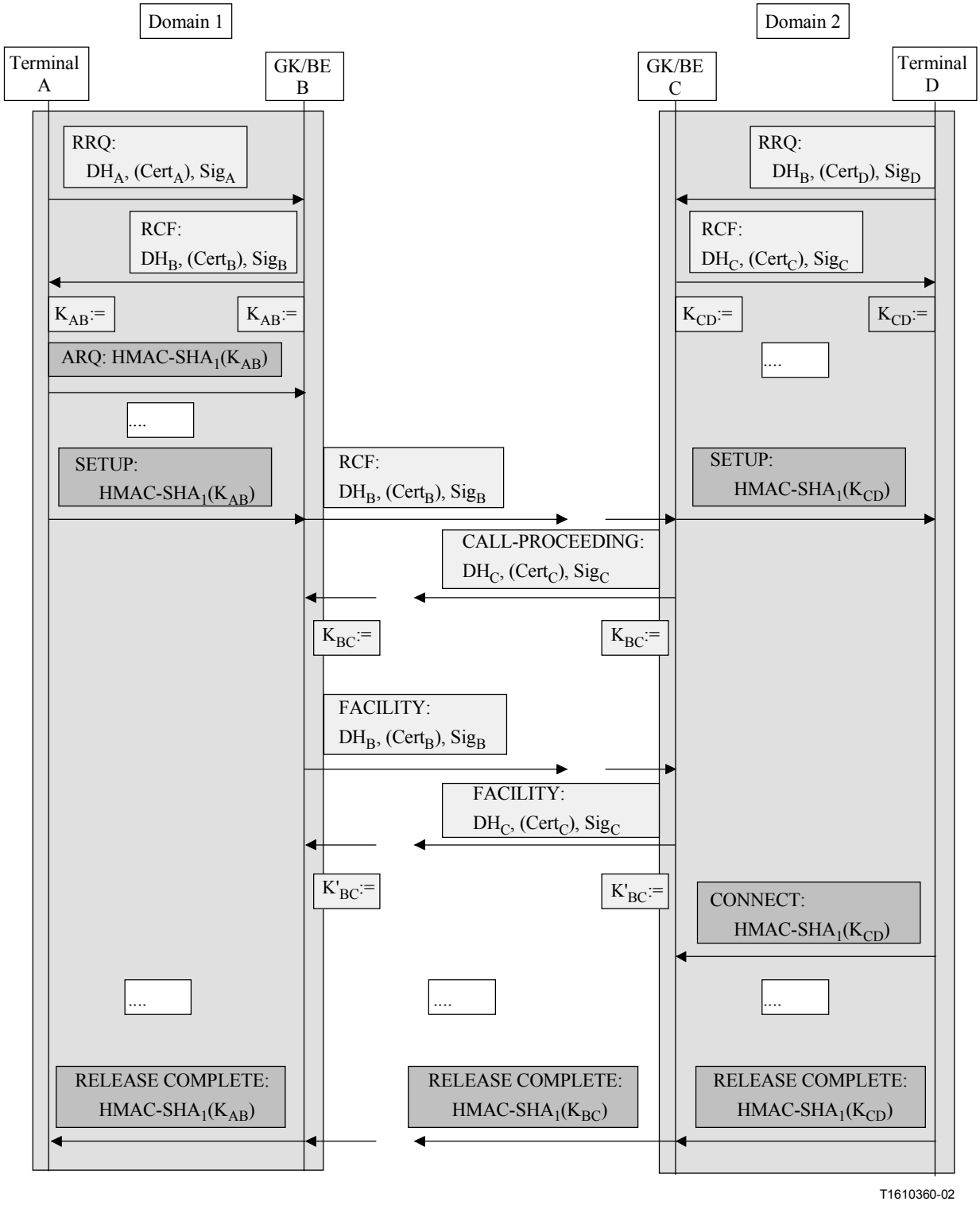


Figure F.3/H.235 – Flow diagram in a multi-administrative domain

F.11 Multicast behavior

H.225.0 multicast messages such as **GRQ** or **LRQ** shall include a **CryptoToken** according to Procedure II where the **generalID** is not set. When such messages are sent unicast, then the message shall include a **CryptoToken** with the **generalID** set.

F.12 List of secure signalling messages

Procedure IV deploys Procedure I of Annex D or Procedure II of Annex E, depending on the scenario and on the actual message, as indicated below.

F.12.1 H.225.0 RAS

H.225.0 RAS message	H.235 signalling fields	Authentication and integrity	non-repudiation
GatekeeperRequest, GatekeeperConfirm, GatekeeperReject if GK discovery is applied RegistrationRequest, RegistrationConfirm, RegistrationReject if GK discovery is not applied	CryptoToken, ClearToken	Procedure II	Procedure II
Any other RAS message (Note 2)	CryptoToken	Procedure I	
NOTE 1 – For unicast messages, procedures II shall be applied with the security fields in the **CryptoToken** used. NOTE 2 – GK discovery and multicast messages are not sent.			

F.12.2 H.225.0 call signalling (single administrative domain)

H.225.0 Call Signalling message	H.235 signalling fields	Authentication and integrity	Non-repudiation
Setup-UUIE, Connect-UUIE[a)], Facility-UUIE[b)], Alerting-UUIE, CallProceeding-UUIE, Facility-UUIE, Progress-UUIE, Information-UUIE, ReleaseComplete-UUIE, Status-UUIE, StatusInquiry-UUIE, SetupAcknowledge-UUIE, Notify-UUIE	CryptoToken, ClearToken	Procedure I	
Facility-UUIE[c)]	CryptoToken	Procedure II	Procedure II
a) Assuming that either message is the first in each direction. b) Not used for key update. c) Used for key update.			

F.12.3 H.225.0 call signalling (multi-administrative domain)

H.225.0 Call Signalling message	H.235 signalling fields	Authentication and integrity	Non-repudiation
Setup-UUIE, Connect-UUIE[a)], Alerting-UUIE[b)], CallProceeding-UUIE, Facility-UUIE[c)], Progress-UUIE, Information-UUIE, ReleaseComplete-UUIE	CryptoToken, ClearToken	Procedure II	Procedure II
Alerting-UUIE[d)], CallProceeding-UUIE, Facility-UUIE[e)], Progress-UUIE, Information-UUIE, ReleaseComplete-UUIE, Status-UUIE, StatusInquiry-UUIE, SetupAcknowledge-UUIE, Notify-UUIE	CryptoToken, ClearToken	Procedure I	Procedure I

a) Assuming that either message is the first in each direction.

b) Any of those messages occurs as first message in either direction.

c) used for key update.

d) Any of those messages does not occur as the first message in either direction.

e) Not used for key update.

F.13 List of Object Identifiers

Table F.2 lists all the referenced OIDs.

Table F.2/H.235 – Object Identifiers used by Annex F

Object Identifier Reference	Object Identifier Value(s)	Description
"A1"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 20}	Used as replacement for OID "A" in procedure II of Annex E for the CryptoToken-tokenOID indicating that the RSA signature/hash includes all fields in the RAS/H.225.0 message (authentication and integrity).
"S1"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 21}	Used as replacement for OID "S" in procedure II of Annex E for the ClearToken-tokenOID indicating that the ClearToken is being used for message authentication and integrity. This OID in the end-to-end CryptoToken implicitly indicates also use of DH during fast start.
"Q"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 22}	Used in procedure IV indicating that the ClearToken on the hop-by-hop link carries a Diffie-Hellman token .
"W"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 23}	Used in procedure IV as algorithm OID indicating use of an RSA SHA1-based digital signature.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
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	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
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 and open system communications
Series Y	Global information infrastructure and Internet protocol aspects
Series Z	Languages and general software aspects for telecommunication systems

Geneva, 2002