INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

H.235 Implementors' Guide

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(5 August 2005)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Systems aspects

Implementors Guide for H.235 V3: "Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals"

Summary

This document is a compilation of reported defects identified in Version 3 of ITU-T Recommendation H.235, which comprises: H.235 (2003-08), H.235 Corrigendum 1 (2005-01), H.235 Amendment 1 (2004-04) and H.235 Amendment 2 (2005-01). It must be read in conjunction with the Recommendations to serve as an additional authoritative source of information for implementers.

It should be noted that H.235 V3 has been superseded by H.235 V4, and this Implementors' Guide is provided solely as assistance to implementors of H.235 V3. The changes, clarifications and corrections defined herein have been included in H.235 V4.

In particular, this Implementors' Guide addresses errors found in H.235 (2003) Annex D, in H.235 (2004) Amendment 1 Annex H and in Annex I.

This Implementors' Guide contains all updates submitted upto and including those at Study Group 16 meeting, July/August 2005, in Geneva (TD 147/PLEN), and was approved on 5 August 2005.

Contact Information

ITU-T Study Group 16 / Rapporteur Question 25/16	Martin Euchner Siemens AG Hofmannstr 51 81359 Munich, Germany	Tel: Fax: E-mail:	+49 89 722 5 57 90 +49 89 722 6 23 66 martin.euchner@siemens.com
Editor ITU-T Rec. H.235	Martin Euchner Siemens AG Hofmannstr 51 81359 Munich, Germany	Tel: Fax: E-mail:	+49 89 722 5 57 90 +49 89 722 6 23 66 martin.euchner@siemens.com

Table of Contents

IMPLEMENTORS' GUIDE FOR ITU-T H.235: "SECURITY AND ENCRYPTION FOR H-SERIES (H.323 AND OTHER H.245-BASED) MULTIMEDIA TERMINALS"

1 Introduction

This document is a compilation of reported defects identified in Version 3 of ITU-T Recommendation H.235 (2003-08) and its Corrigendum 1 (2005-01) and Amendments 1 (2004-04) and 2 (2005-01). It should be noted that H.235 V3 has been superseded by H.235 V4, and this Implementors' Guide is provided solely as assistance to implementors of H.235 V3. It must be read in conjunction with the Recommendations to serve as an additional authoritative source of information for implementers. The changes, clarifications and corrections defined herein have been included in H.235 V4.

Upon discovering technical defects with any components of H.235 Version 3, please provide a written description directly to the editor of the Recommendation, with copy to the Rapporteur of Q.25/16. The template for a defect report is located at the end of the Guide. Contact information for these parties is included at the front of the document. Return contact information should also be supplied so a dialogue can be established to resolve the matter and an appropriate reply to the defect report can be conveyed. This defect resolution process is open to any interested party. Formal membership in the ITU is not required to participate in this process.

2 Scope

This guide resolves defects in the following categories:

- editorial errors
- technical errors, such as omissions and inconsistencies
- ambiguities

In addition, the Implementors' Guide may include explanatory text found necessary as a result of interpretation difficulties apparent from the defect reports.

This Guide will not address proposed additions, deletions, or modifications to the Recommendations that are not strictly related to implementation difficulties in the above categories. Proposals for new features should be made in through contributions to the ITU-T.

3 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 Recommendation H.235 (2003-08), Security and encryption for H Series (H.323 and other H.245 based) multimedia terminals

– ITU-T Recommendation H.235 (2003) Amendment 1 (2004-04)

- ITU-T Recommendation H.235 (2003) Amendment 2 (2005-01) “Annex G: Usage of the MIKEY key management protocol for the secure real time transport protocol (SRTP) within H.235"
- ITU-T Recommendation H.235 (2003) Corrigendum 1 (01/05)

4 Nomenclature

In addition to traditional revision marks, the following marks and symbols are used to indicate to the reader how changes to the text of a Recommendation should be applied:

Symbol	Description
[Begin Correction]	Identifies the start of revision marked text based on extractions from the published Recommendations affected by the correction being described.
[End Correction]	Identifies the end of revision marked text based on extractions from the published Recommendations affected by the correction being described.
...	Indicates that the portion of the Recommendation between the text appearing before and after this symbol has remained unaffected by the correction being described and has been omitted for brevity.
--- SPECIAL INSTRUCTIONS --- {instructions}	Indicates a set of special editing instructions to be followed.

5 Technical and Editorial Corrections to H.323 Series Recommendations

5.1 Corrections to H.235 (2003) Annex D “Baseline security profile”

Description:	The current text describing the detection of the use of Procedure I supplied in Note 7 is incorrect. The text below supplies the correction.

[Begin Correction]

…

D.6.3.2 Symmetric-key-based signalling message authentication details (procedure I)

…

NOTE 7 – The recipient is able to detect usage of procedure I by evaluating the **tokenOID** within the hashed **EncodedGeneralToken** (detecting presence of "A~~B~~").

…

[End Correction]

5.2 Corrections to H.235 (2003) Annex H "Framework for secure authentication in RAS using weak shared secrets"

Description:	The size of initialization vector used in the Symmetric Encryption algorithm for SP1 specified in Annex H.7/H.235 Amendment 1 is incorrect. The text below supplies the correction.

[Begin Correction]

…

H.7 A Specific Security Profile (SP1)

…

- Master key, K_m, negotiation: Diffie-Hellman key exchange using the OAKLEY well-known group 2 [RFC 2412], followed by the SHA1 hash reduction of the Diffie-Hellman secret: K_m = SHA1(Diffie-Hellman shared secret).
- Symmetric encryption algorithm: shall be AES-128 in segmented counter mode with a 2-octet party discriminator, D, a 124-octet initialization vector, IV, and a 2-octet counter field, C, such that counter = D || IV || C, and C = 0 initially. See [NIST 800-38A] for a description of CTR mode. The party discriminator, D, is set to 0x3636 when the IV is generated by the party which issued the GRQ/RRQ, or LRQ, and is set to 0x5c5c when the IV is generated by the party which responded with GCF/RCF, or LCF. Each party must insure that each IV it generates is unique; it may use its own method to insure this uniqueness.
- Diffie-Hellman key encryption: shall use the AES-128 segmented counter mode to encrypt the Diffie-Hellman public key (represented as an octet string in network byte order); the initialization vector shall be carried in **ClearToken.initVect,** and the 16-octet key, K_p, shall be constructed as the high-order 128 bits of the SHA1 hash of the user password: K_p = Trunc(SHA1(user password), 16), where Trunc(x,y) truncates octet string x to y octets. Note that this is typically considered a weak key.

…

[End Correction]

5.3 Corrections to H.235 (2003) Annex I "Support of direct-routed calls"

Description:	The text below provides various corrections to the Procedure DRC specified in Annex I/H.235 Amendment 1 and Annex I/H.235 Corrigendum 1.

[Begin Correction]

…

I.9 Procedure DRC

…

Gatekeeper H shall generate a random Challenge-B, encryption key material EK_{BH} and salting key material KS_{BH} from the shared secret K_{BH} using the PRF-**based** key derivation procedure as defined in I.10 where Challenge-B is substituted as **challenge** and CT_{HG}**→h235Key→~~V3KeySyncMaterial→~~secureSharedSecret→keyDerivationOID** shall hold "AnnexI-HMAC-SHA1-PRF"; see I.12.

EK_{GH} denotes the encryption key and KS_{GH} denotes the salting key that are shared between gatekeeper G and gatekeeper H. Gatekeeper H shall generate one random Challenge-G. Gatekeeper H shall generate encryption key material EK_{GH} and salting key material KS_{GH} from the shared secret K_{GH} using the PRF-based key derivation procedure as defined in clause 11 where Challenge-G is substituted for **challenge**. CT_{HG}**→challenge** shall hold challenge-G, the endpoint ID of the endpoint B shall be set in CT_{HG}**→h235Key~~→V3KeySyncMaterial~~→secureSharedSecret→generalID.**

Gatekeeper H shall transmit the encrypted EK_{BH} and the encrypted KS_{BH} to gatekeeper G. The enhanced OFB (EOFB) encryption mode (see B.2.5) shall be used with the secret, endpoint-specific salting key KS_{GH}. Applicable encryption algorithms are (see D.11):

…

For the EOFB encryption mode, gatekeeper H shall generate a random initial value IV. For OID "X1", OID "Y1" and OID "Z1" the IV has 64 bits and shall be conveyed within CT_{HG}**→h235Key~~→V3KeySyncMaterial~~→secureSharedSecret→params→iv8;** whereas the IV has 128 bits for OID "Z2" and shall be conveyed within CT_{HG}**→h235Key~~→V3KeySyncMaterial~~→secureSharedSecret→params→iv16**.

Gatekeeper H shall include $ENC_{EK_{GH}, KS_{GH}, IV}(EK_{BH})$ and $ENC_{EK_{GH}, KS_{GH}, IV}(KS_{BH})$ in ClearToken CT_{HG} with **tokenOID** set to "I3". The obtained ciphertext $ENC_{EK_{GH}, KS_{GH}, IV}(EK_{BH})$ shall be conveyed in CT_{HG}**→h235Key~~→V3KeySyncMaterial~~→secureSharedSecret→encryptedSessionKey**; the obtained ciphertext $ENC_{EK_{GH}, KS_{GH}, IV}(KS_{BH})$ shall be conveyed in CT_{HG}**→h235Key→secureSharedSecret→encryptedSaltingKey**. The encryption algorithm shall be indicated in CT_{HG}**→h235Key→~~V3KeySyncMaterial→~~algorithmOID** ("X1", "Y1", "Z1" or "Z2"). Challenge-B shall be placed within CT_{HG}**→h235Key→~~V3KeySyncMaterial~~→secureSharedSecret→clearSaltingKey**. CT_{HG}**→generalID** shall be set to the gatekeeper identifier G wheras CT_{HG}**→sendersID** shall be set to the gatekeeper identifier H.

Challenge-B shall be conveyed to endpoint B by inclusion of a **profileInfo** within the **ClearToken** CT_{HG}**→profileInfo→elementID** = 0 that identifies this particular profile element;

CT_{HG}**→profileInfo→paramS** left unused and CT_{HG}**→profileInfo→element→octets** shall hold Challenge-B.

The **LCF** response shall hold the ClearToken CT_{HG}.

…

Two ClearTokens shall be included, one CT_A for the caller A and another one CT_B for the callee B. Each **ClearToken** shall contain an OID ("I1" or "I2") within **tokenOID** that indicates whether the token is destined for the caller (OID "I1" for CT_A) or for the callee (OID "I2" for CT_B).

GK G shall decrypt CT_{HG}**→h235Key→secureSharedSecret→encryptedSessionKey** to obtain EK_{BH} and shall decrypt CT_{HG}**→h235Key→secureSharedSecret→encryptedSaltingKey** to obtain KS_{BH}.

The **ClearToken** as defined in this annex may be used in conjunction with other security profiles such as with Annex D or with Annex F that deploy **ClearTokens** as well.

…

The encryption keys EK$_{AG}$ and EK$_{BH}$ for the encrypted end-to-end key K$_{AB}$ shall be derived from the shared secret between the gatekeeper and the endpoints (EK$_{AG}$ or EK$_{BH}$) using the PRF-**based** key derivation procedure as defined in clause I.10 where both CT$_A$→**h235Key**→~~**V3KeySyncMaterial**~~→**secureSharedSecret**→**keyDerivationOID** and CT$_B$→**h235Key**→~~**V3KeySyncMaterial**~~→**secureSharedSecret**→**keyDerivationOID** shall hold "Annex I-HMAC-SHA1-PRF", see clause I.12 and CT$_A$→**challenge** shall hold Challenge-A.

Gatekeeper G shall copy Challenge-B from CT$_{HG}$→**h235Key**→~~**V3KeySyncMaterial**~~→**secureSharedSecret**→**clearSaltingKey** into CT$_B$→**challenge**.

CT$_B$→**profileInfo** shall hold the profile element that was conveyed in CT$_{HG}$ **profileInfo** such that in the end endpoint B obtains Challenge-B.

This session secret K$_{AB}$ shall be encrypted by EK$_{AG}$ (for CT destined to endpoint A) or by EK$_{BH}$ (for the CT destined to endpoint B) using an encryption algorithm.

…

For the EOFB encryption mode, the gatekeeper G shall generate a random initial value IV. For OID "X1", OID "Y1" and OID "Z1" the IV has 64 bits and shall be conveyed within CT$_A$→**h235Key**→~~**V3KeySyncMaterial**→~~**secureSharedSecret**→**params**→**iv8** and within CT$_B$→**h235Key**→~~**V3KeySyncMaterial**~~→**secureSharedSecret**→**params**→**iv8;** whereas the IV has 128 bits for OID "Z2" and shall be conveyed within CT$_A$→**h235Key**~~→**V3KeySyncMaterial**~~→**secureSharedSecret**→**params**→**iv16** and within CT$_B$→**h235Key**~~→**V3KeySyncMaterial**~~→**secureSharedSecret**→**params**→**iv16**.

The obtained ciphertext ENC$_{EK_{AG}, KS_{AG}, IV}$(K$_{AB}$) shall be conveyed in CT$_A$→**h235Key**~~→**V3KeySyncMaterial**~~→**secureSharedSecret**→**encryptedSessionKey** and ENC$_{EK_{BH}, KS_{BH}, IV}$(K$_{AB}$) shall then be conveyed in CT$_B$→**h235Key**→~~**V3KeySyncMaterial**~~→**secureSharedSecret**→**encryptedSessionKey**. The encryption algorithm shall be indicated in CT$_A$→**h235Key**→~~**V3KeySyncMaterial**~~→**secureSharedSecret**→**algorithmOID** and in CT$_B$→**h235Key**→~~**V3KeySyncMaterial**~~→**secureSharedSecret**→**algorithmOID** ("X1", "Y1", "Z1" or "Z2").

For the ClearToken destined to endpoint A, the endpoint identifier of endpoint B (EPID$_B$) shall be placed within CT$_A$→**h235Key**→~~**V3KeySyncMaterial**~~→**secureSharedSecret**→**generalID**. Likewise for the ClearToken destined to endpoint B, the endpoint identifier of endpoint A (EPID$_A$) shall be placed within CT$_B$→**h235Key**→~~**V3KeySyncMaterial**~~→**secureSharedSecret**→**generalID**.

…

If the received CT$_A$ was verified as being fresh, endpoint A shall retrieve the IV and compute EK$_{AG}$ and KS$_{AG}$ as described above for the gatekeeper G. Endpoint A shall decrypt the **encryptedSessionKey** information found within **secureSharedSecret**~~**V3KeySyncMaterial**~~ of CT$_A$ to obtain K$_{AB}$.

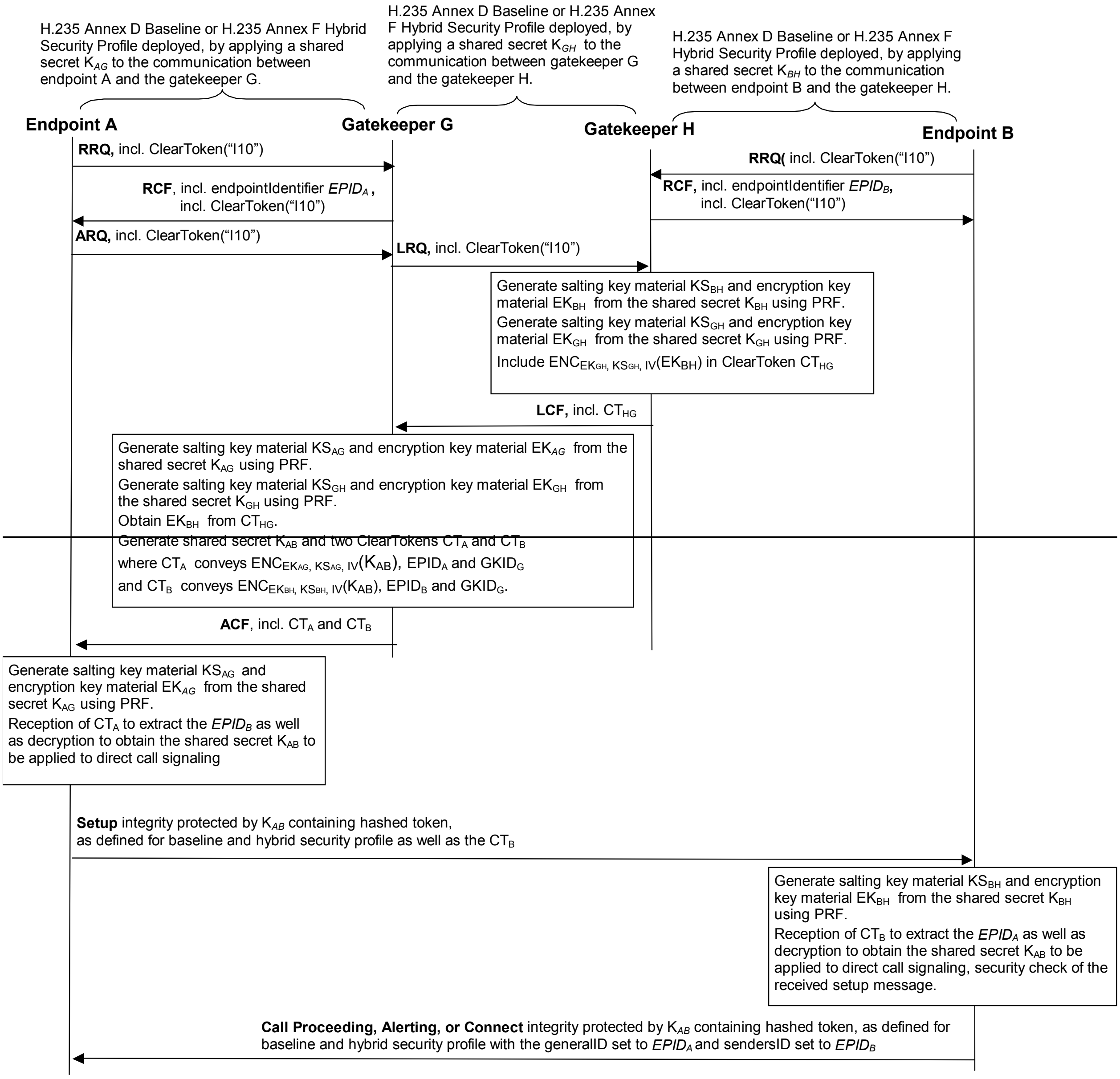
…

Endpoint B shall verify that the obtained CT$_B$ is fresh by checking the **timestamp**. Further security checks shall verify the **sendersID** of the ClearToken and **generalID** within **secureSharedSecret**~~**V3KeySyncMaterial**~~. If the received CT$_B$ was verified as being fresh, endpoint B shall retrieve Challenge-B from CT$_{HG}$→**profileInfo**→**element**→**octets**, and retrieve the

IV and compute EK_{BHG} and KS_{BH}~~-~~, Challenge-B substituted as **challenge** in clause I.10 as described above for the gatekeeper. Endpoint B shall decrypt the **encryptedSessionKey** information found within **secureSharedSecret**~~**V3KeySyncMaterial**~~ of CT_B to obtain K_{AB}.

In case CT_B was verified as being fresh, endpoint B is able to proceed the call signalling by replying with CALL-PROCEEDING, ALERTING or CONNECT etc., as appropriate.

…


H.235 Annex D Baseline or H.235 Annex F Hybrid Security Profile deployed, by applying a shared secret K_{AG} to the communication between endpoint A and the gatekeeper G.
H.235 Annex D Baseline or H.235 Annex F Hybrid Security Profile deployed, by applying a shared secret K_{GH} to the communication between gatekeeper G and the gatekeeper H.
H.235 Annex D Baseline or H.235 Annex F Hybrid Security Profile deployed, by applying a shared secret K_{BH} to the communication between endpoint B and the gatekeeper H.
Endpoint A
Gatekeeper G
Gatekeeper H
Endpoint B
RRQ, incl. ClearToken("I10")
RRQ(incl. ClearToken("I10")
RCF, incl. endpointIdentifier $EPID_A$, incl. ClearToken("I10")
RCF, incl. endpointIdentifier $EPID_B$, incl. ClearToken("I10")
ARQ, incl. ClearToken("I10")
LRQ, incl. ClearToken("I10")
Generate salting key material KS_{BH} and encryption key material EK_{BH} from the shared secret K_{BH} using PRF.
Generate salting key material KS_{GH} and encryption key material EK_{GH} from the shared secret K_{GH} using PRF.
Include $ENC_{EK_{GH}, KS_{GH}, IV}(EK_{BH})$ in ClearToken CT_{HG}
LCF, incl. CT_{HG}
Generate salting key material KS_{AG} and encryption key material EK_{AG} from the shared secret K_{AG} using PRF.
Generate salting key material KS_{GH} and encryption key material EK_{GH} from the shared secret K_{GH} using PRF.
Obtain EK_{BH} from CT_{HG}.
Generate shared secret K_{AB} and two ClearTokens CT_A and CT_B
where CT_A conveys $ENC_{EK_{AG}, KS_{AG}, IV}(K_{AB})$, $EPID_A$ and $GKID_G$
and CT_B conveys $ENC_{EK_{BH}, KS_{BH}, IV}(K_{AB})$, $EPID_B$ and $GKID_G$.
ACF, incl. CT_A and CT_B
Generate salting key material KS_{AG} and encryption key material EK_{AG} from the shared secret K_{AG} using PRF.
Reception of CT_A to extract the $EPID_B$ as well as decryption to obtain the shared secret K_{AB} to be applied to direct call signaling
Setup integrity protected by K_{AB} containing hashed token, as defined for baseline and hybrid security profile as well as the CT_B
Generate salting key material KS_{BH} and encryption key material EK_{BH} from the shared secret K_{BH} using PRF.
Reception of CT_B to extract the $EPID_A$ as well as decryption to obtain the shared secret K_{AB} to be applied to direct call signaling, security check of the received setup message.
Call Proceeding, Alerting, or Connect integrity protected by K_{AB} containing hashed token, as defined for baseline and hybrid security profile with the generalID set to $EPID_A$ and sendersID set to $EPID_B$

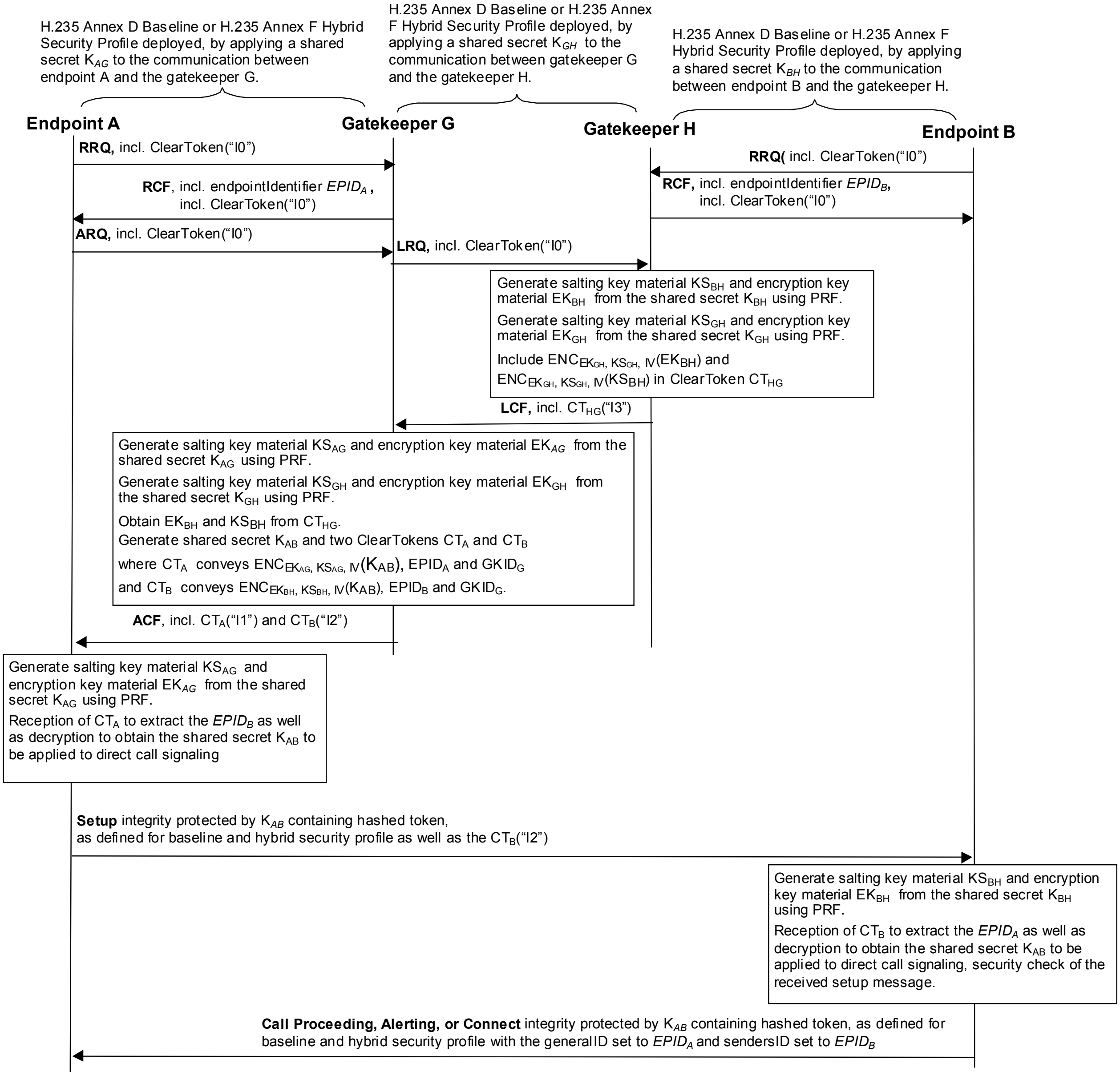

H.235 Annex D Baseline or H.235 Annex F Hybrid Security Profile deployed, by applying a shared secret K_{AG} to the communication between endpoint A and the gatekeeper G.
H.235 Annex D Baseline or H.235 Annex F Hybrid Security Profile deployed, by applying a shared secret K_{GH} to the communication between gatekeeper G and the gatekeeper H.
H.235 Annex D Baseline or H.235 Annex F Hybrid Security Profile deployed, by applying a shared secret K_{BH} to the communication between endpoint B and the gatekeeper H.
Endpoint A
Gatekeeper G
Gatekeeper H
Endpoint B
RRQ, incl. ClearToken(“I0”)
RRQ(incl. ClearToken(“I0”)
RCF, incl. endpointIdentifier $EPID_A$, incl. ClearToken(“I0”)
RCF, incl. endpointIdentifier $EPID_B$, incl. ClearToken(“I0”)
ARQ, incl. ClearToken(“I0”)
LRQ, incl. ClearToken(“I0”)
Generate salting key material KS_{BH} and encryption key material EK_{BH} from the shared secret K_{BH} using PRF.
Generate salting key material KS_{GH} and encryption key material EK_{GH} from the shared secret K_{GH} using PRF.
Include $ENC_{EK_{GH}, KS_{GH}, IV}(EK_{BH})$ and $ENC_{EK_{GH}, KS_{GH}, IV}(KS_{BH})$ in ClearToken CT_{HG}
LCF, incl. CT_{HG}(“I3”)
Generate salting key material KS_{AG} and encryption key material EK_{AG} from the shared secret K_{AG} using PRF.
Generate salting key material KS_{GH} and encryption key material EK_{GH} from the shared secret K_{GH} using PRF.
Obtain EK_{BH} and KS_{BH} from CT_{HG}.
Generate shared secret K_{AB} and two ClearTokens CT_A and CT_B
where CT_A conveys $ENC_{EK_{AG}, KS_{AG}, IV}(K_{AB})$, $EPID_A$ and $GKID_G$
and CT_B conveys $ENC_{EK_{BH}, KS_{BH}, IV}(K_{AB})$, $EPID_B$ and $GKID_G$.
ACF, incl. CT_A(“I1”) and CT_B(“I2”)
Generate salting key material KS_{AG} and encryption key material EK_{AG} from the shared secret K_{AG} using PRF.
Reception of CT_A to extract the $EPID_B$ as well as decryption to obtain the shared secret K_{AB} to be applied to direct call signaling
Setup integrity protected by K_{AB} containing hashed token, as defined for baseline and hybrid security profile as well as the CT_B(“I2”)
Generate salting key material KS_{BH} and encryption key material EK_{BH} from the shared secret K_{BH} using PRF.
Reception of CT_B to extract the $EPID_A$ as well as decryption to obtain the shared secret K_{AB} to be applied to direct call signaling, security check of the received setup message.
Call Proceeding, Alerting, or Connect integrity protected by K_{AB} containing hashed token, as defined for baseline and hybrid security profile with the generalID set to $EPID_A$ and sendersID set to $EPID_B$

Figure I.2/H.235 – Basic communication flow

[End Correction]

Annex: ITU-T Rec. H.235 Version 3 Defect Report Form

DATE:	
CONTACT INFORMATION **NAME:** **COMPANY:** **ADDRESS:** **TEL:** **FAX:** **EMAIL:**	
AFFECTED RECOMMENDATIONS:	
DESCRIPTION OF PROBLEM:	
SUGGESTIONS FOR RESOLUTION:	

NOTE - Attach additional pages if more space is required than is provided above.