INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.530

Corrigendum 1

(07/2003)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Mobility and Collaboration procedures – Security for mobile multimedia systems and services

---

Symmetric security procedures for H.323 mobility in H.510

Corrigendum 1

ITU-T Recommendation H.530 (2002) – Corrigendum 1

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
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.530

Symmetric security procedures for H.323 mobility in H.510

Corrigendum 1

Summary

This corrigendum corrects a security weakness that was identified in ITU-T Rec. H.530 (2002/03) related to the fact that the V-GK cannot verify the received AuthenticationConfirmation message as fresh. This weakness thus enables replay or masquerade attacks. This weakness was corrected by introducing additional security parameters (i.e., parameter W) in the key management response message.

Source

Corrigendum 1 to ITU-T Recommendation H.530 (2002) was approved by ITU-T Study Group 16 (2001-2004) under the ITU-T Recommendation A.8 procedure on 14 July 2003.

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 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.530

Symmetric security procedures for H.323 mobility in H.510

Corrigendum 1

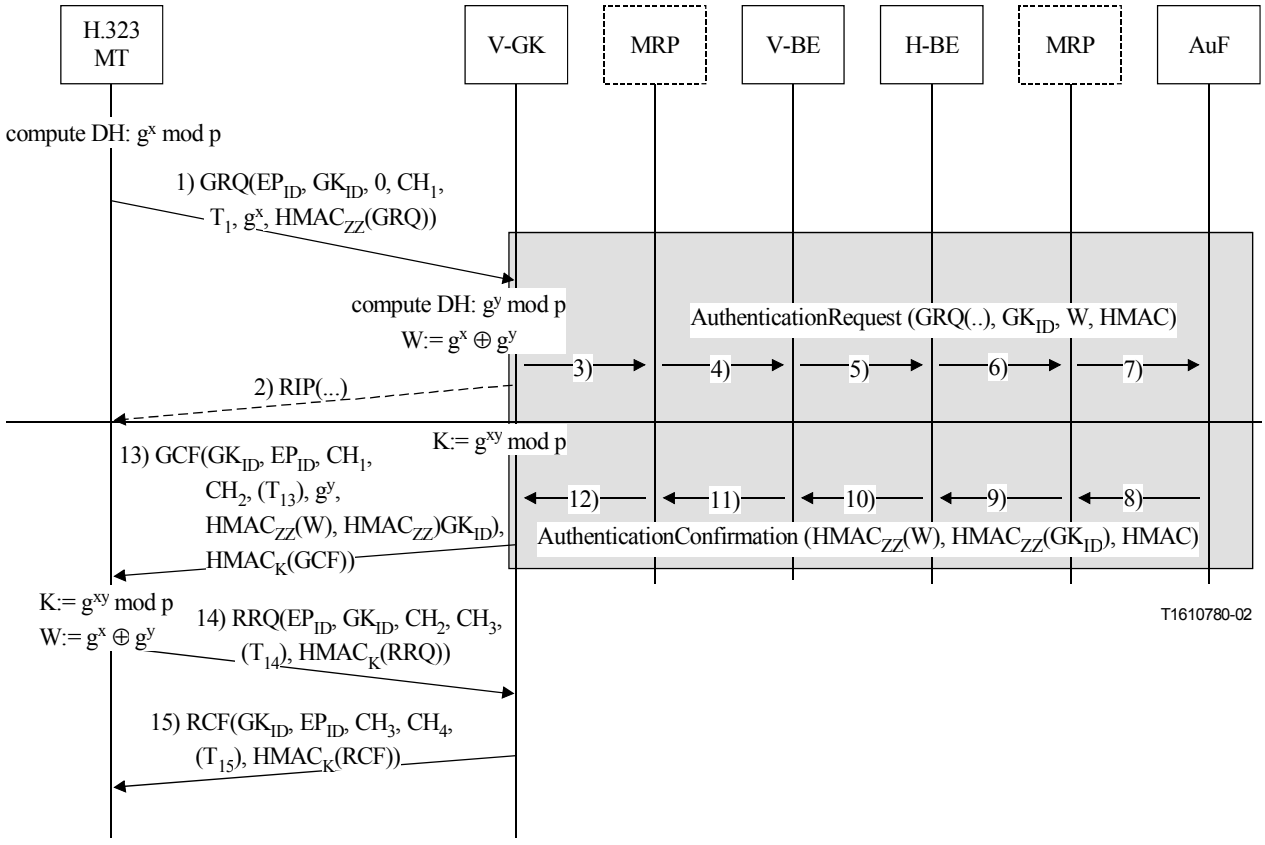
1) Clause 6, References

Add a new reference [8] as follows and update all references to [8] and [9] to [9] and [10], respectively:

[8] ITU-T Recommendation H.235 version 3 (2003), *Security and encryption for H.series (H.323 and other H.245-based) multimedia terminals.*

2) Clause 8.2

a) Replace Figure 2:



With the following:

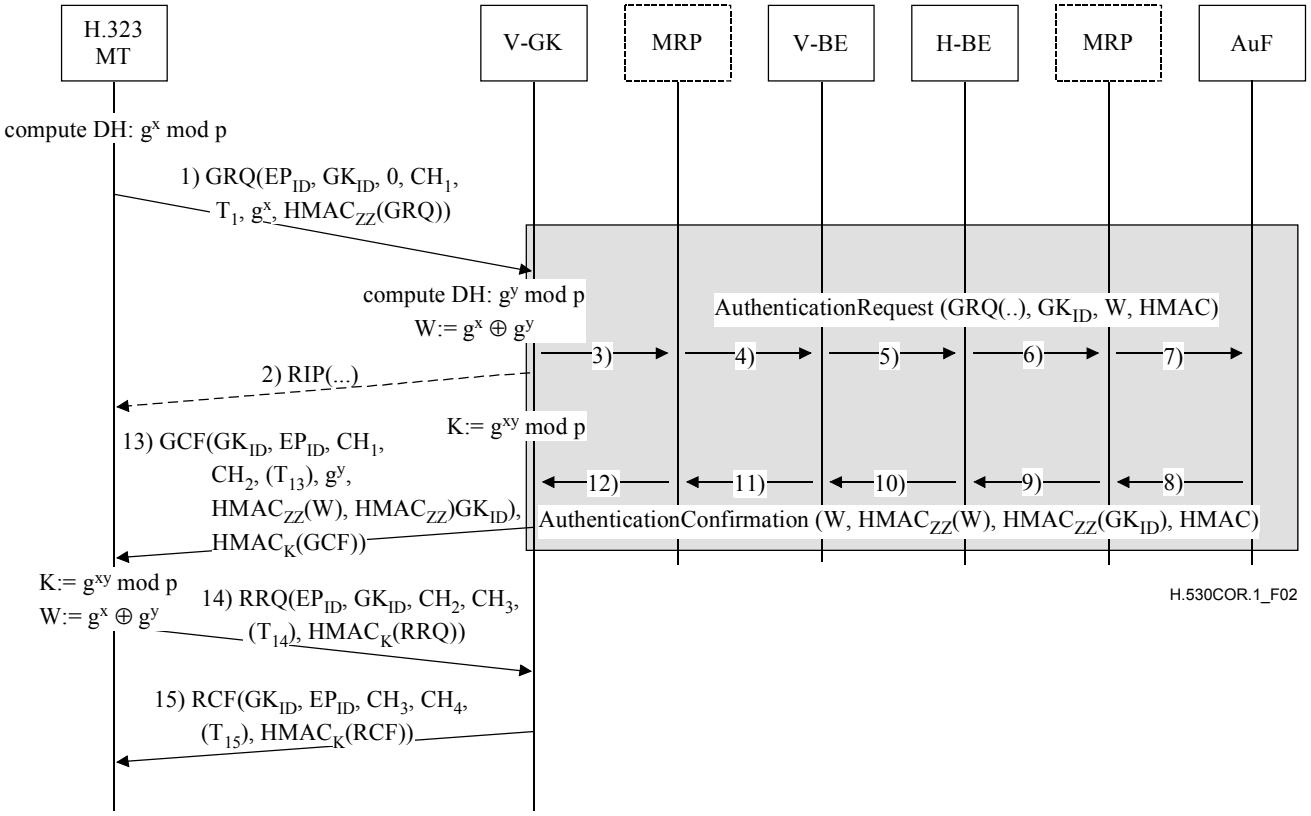
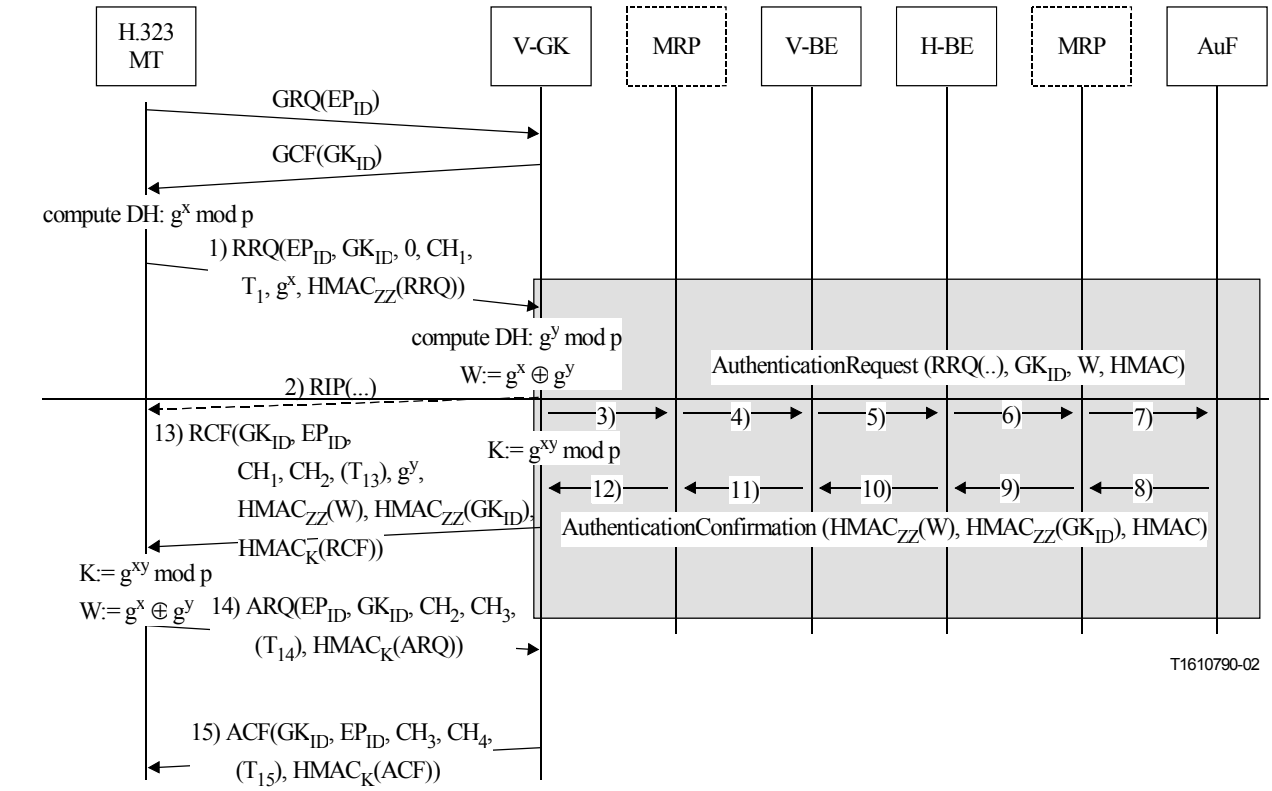


Figure 2/H.530 – Authentication and key management during GK discovery phase

b) Change Figure 3:



With:

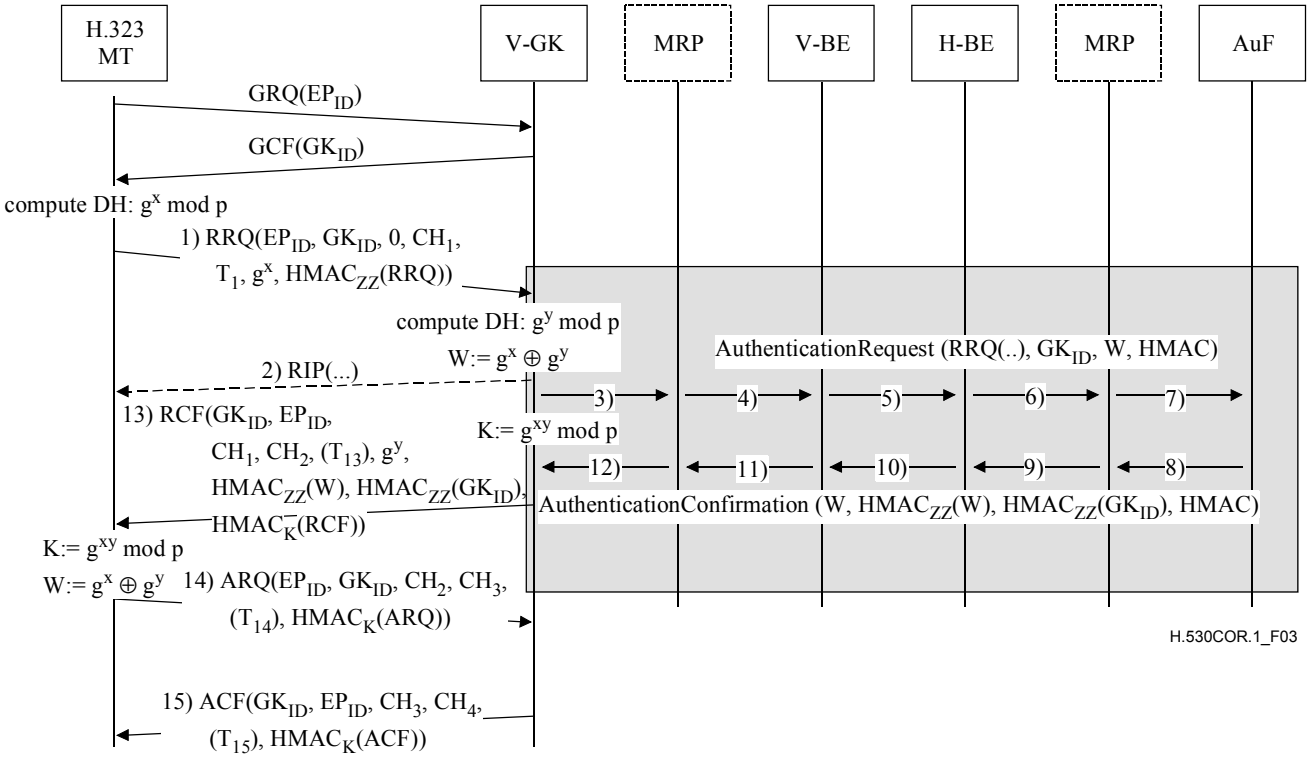


Figure 3/H.530 – Authentication and key management during registration phase

3) Clause 8.2.1

Add the following as indicated:

…

8.2.1 MT to V-GK

…

Until the **RCF** is submitted as message 13), the V-GK has time to compute the dynamic link *K* using the Diffie-Hellman half-key of the MT and its own secret *y*. For HMAC-SHA1-96 message integrity protection of the H.225.0 RAS [1] messages, the 96 leftmost bits shall be taken from the resulting Diffie-Hellman shared secret as represented in network byte order.

The V-GK receives an **AuthenticationConfirmation**/**AuthenticationRejection** with the result of the authentication and authorization check by the AuF and conveyed credentials; see message 12). The V-GK shall verify that the conveyed mobility **ClearToken** holds the same value *W* as was sent in message 3). A mismatch indicates a replay attack; in this case the V-GK shall consider the MT authentication by the AuF as failed and respond with **GRJ**/**RRJ** with **reason** set to securityDenial or other appropriate security error code according to B.2.2/H.235 [8].

The V-GK may supervise reception of **AuthenticationConfirmation**/**AuthenticationRejection** messages using a timer. The timer duration should be chosen long enough by taking the network transit and the AuF processing into account. If the timer expires and the corresponding reply from the AuF has not arrived, the V-GK shall send an unprotected **RCF**.

The V-GK shall generate a new challenge CH_2 and build **RCF**. The **RCF** shall convey the previous challenge CH_1 within **password**, a new challenge CH_2 within **challenge** within the **ClearToken** inside the **CryptoToken** of **RCF**. That **ClearToken** shall also convey the computed Diffie-

Hellman half-key of the V-GK in the **halfkey** field of the **dhkey** field within the **ClearToken** of that message. The applied prime number shall be included in **modsize** while the DH-generator shall be included in **generator** of that **ClearToken**.

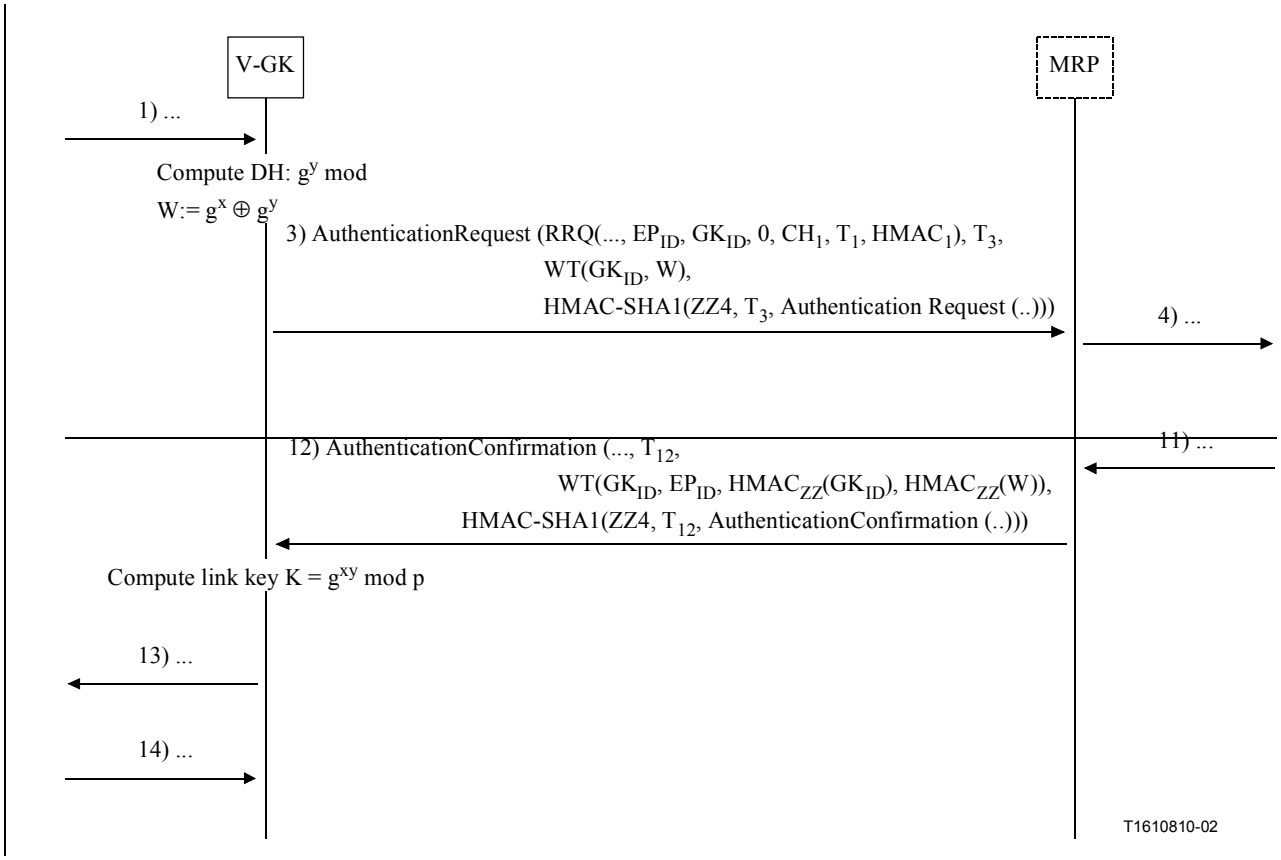
Further, the V-GK shall forward the credentials from the AuF to the MT. The credentials encompass the mobility **ClearToken** shown as **WT()**. This mobility **ClearToken** conveys on one hand the authenticated compound value *W* in the **halfkey** field of the **dhkey** field and on the other hand the authenticated V-GK ID; the value *W* should not be part of forwarded **WT()**. The **tokenOID** shall be set to "G2" and any other parameters in that mobility **ClearToken** shall be unused.

The V-GK computes the HMAC upon the entire **RCF** message using the link key *K*. Thus, the HMAC serves as a response to the previous challenge according to Annex D/H.235 procedure I [4], see message 13).

…

4) Clause 8.2.2

Replace Figure 5:



With:

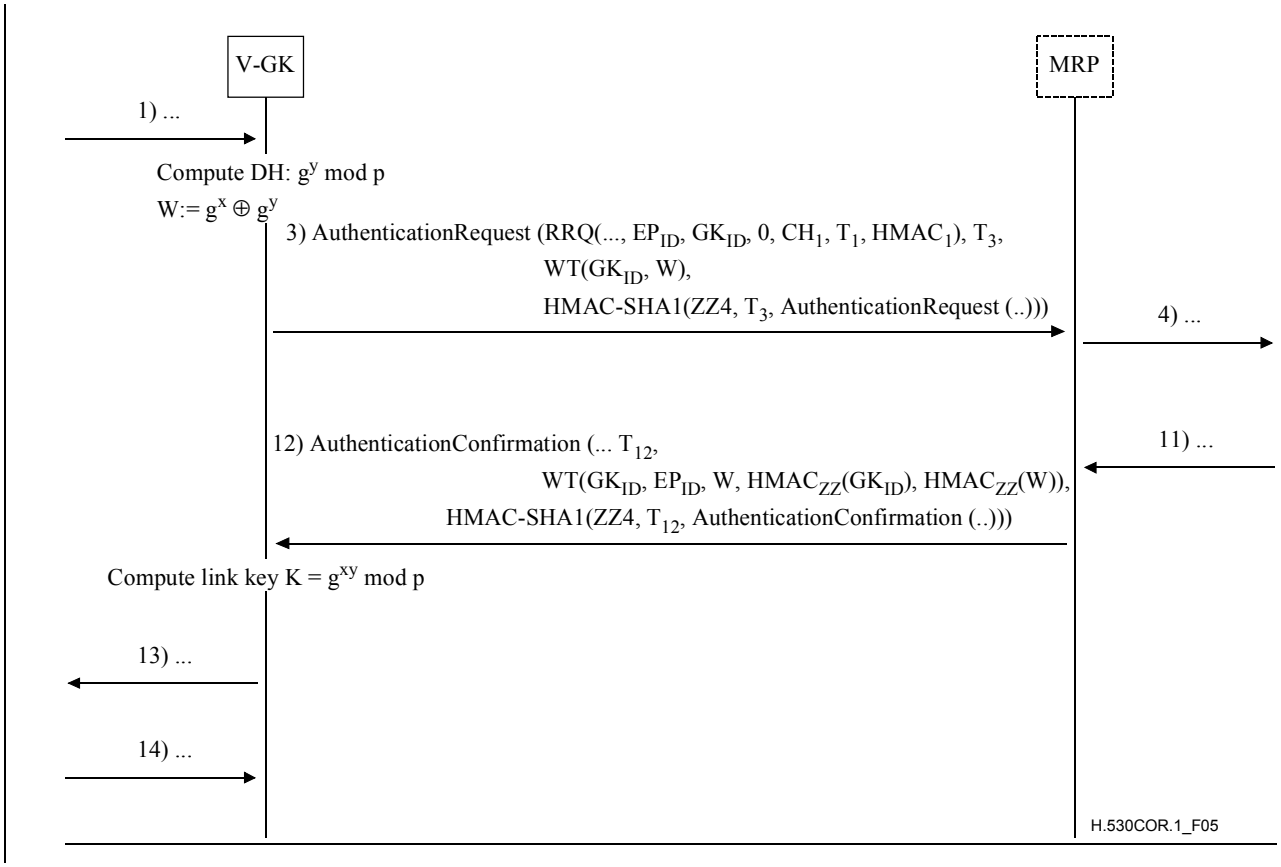
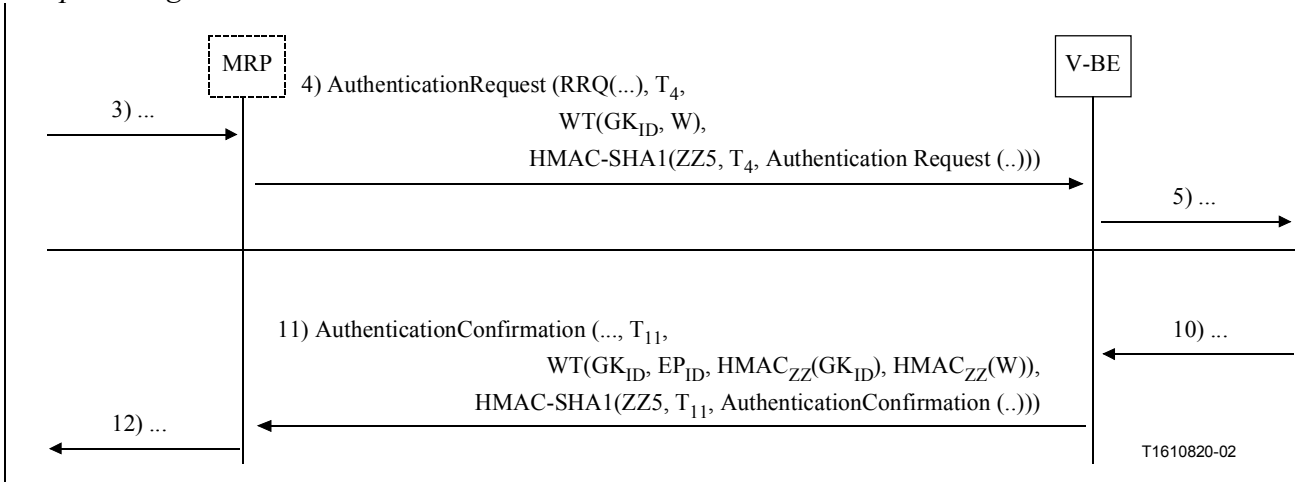


Figure 5/H.530 – Transmission of authentication information between V-GK and MRP

5) Clause 8.2.3

Replace Figure 6:



With:

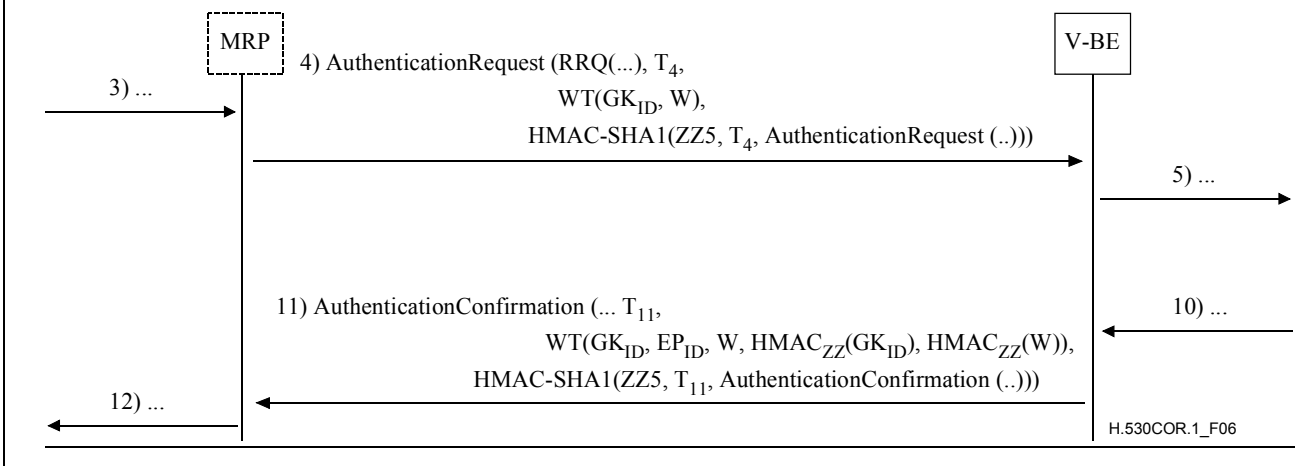
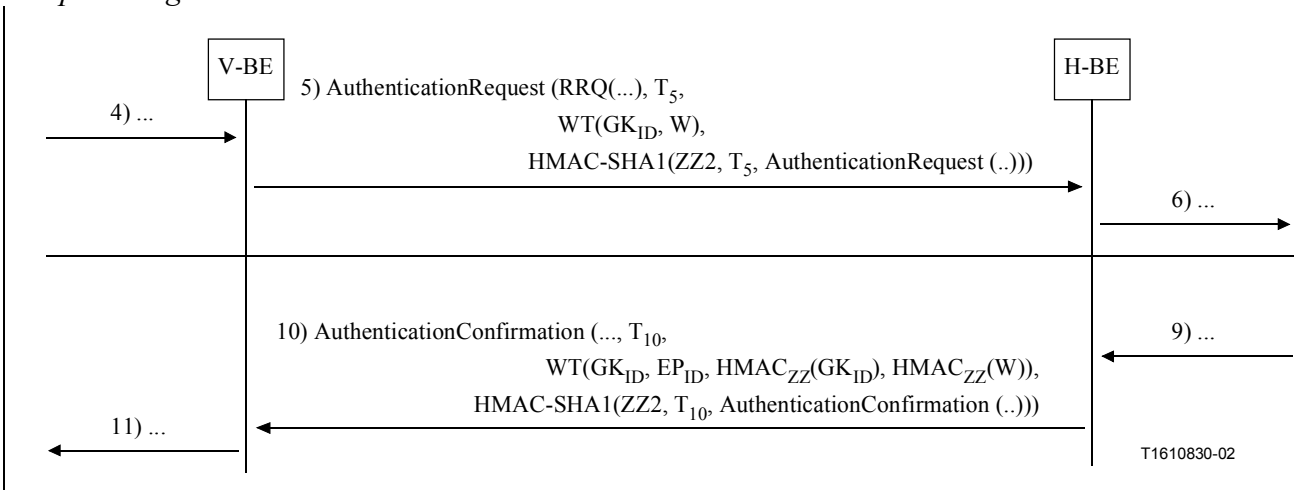


Figure 6/H.530 – Transmission of authentication information between MRP and V-BE

6) Clause 8.2.4

Replace Figure 7:



With:

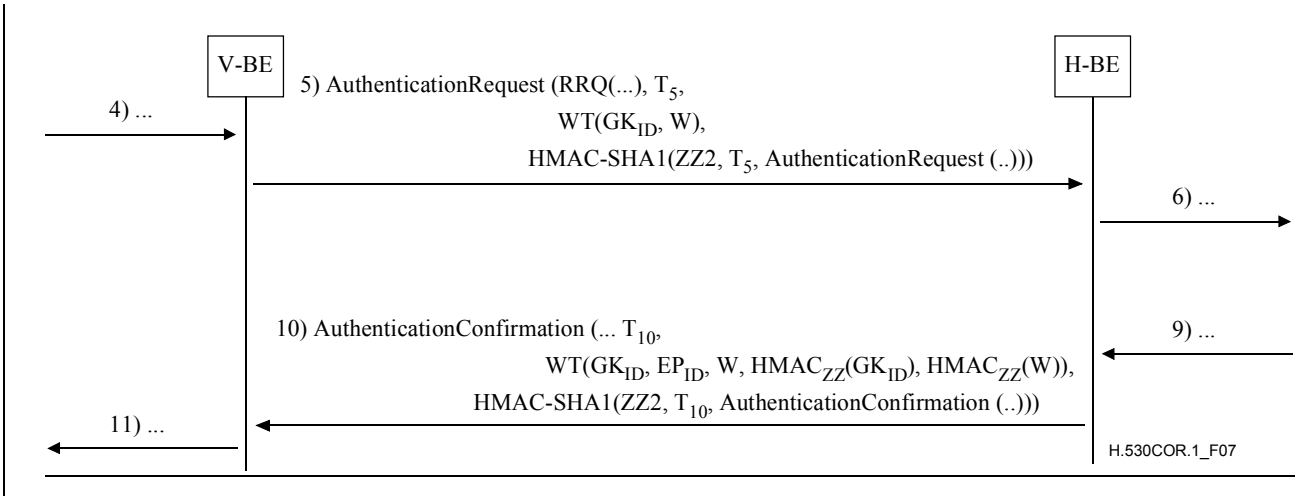
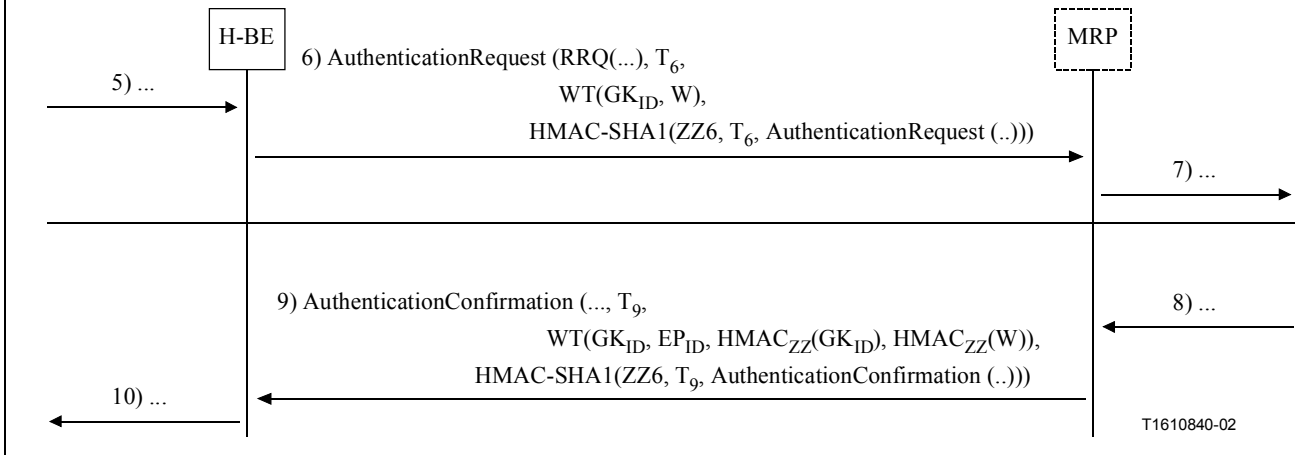


Figure 7/H.530 – Transmission of authentication information between BEs

7) Clause 8.2.5

Replace Figure 8:



With:

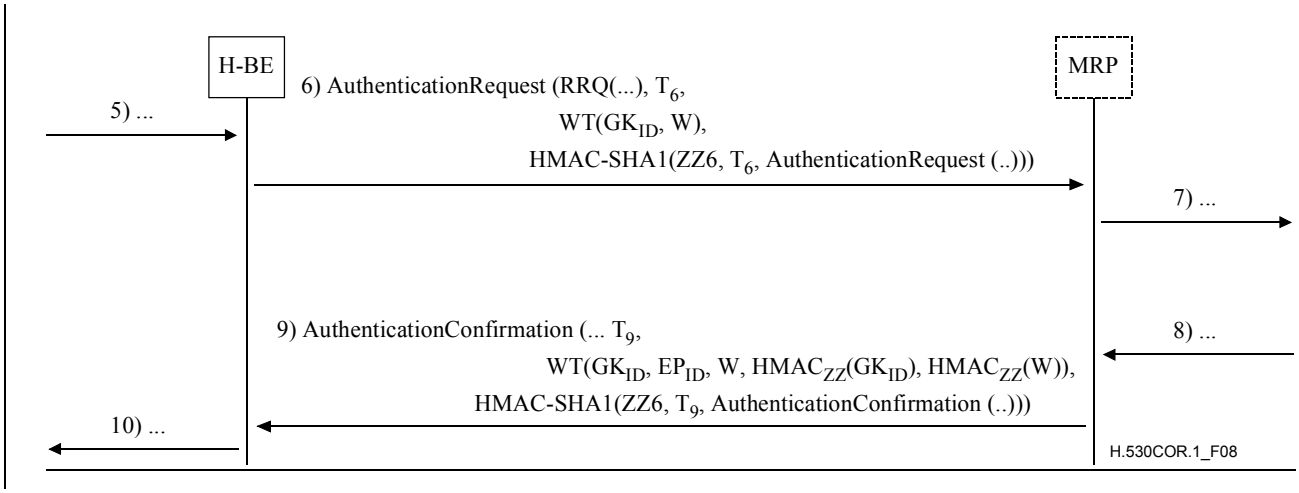
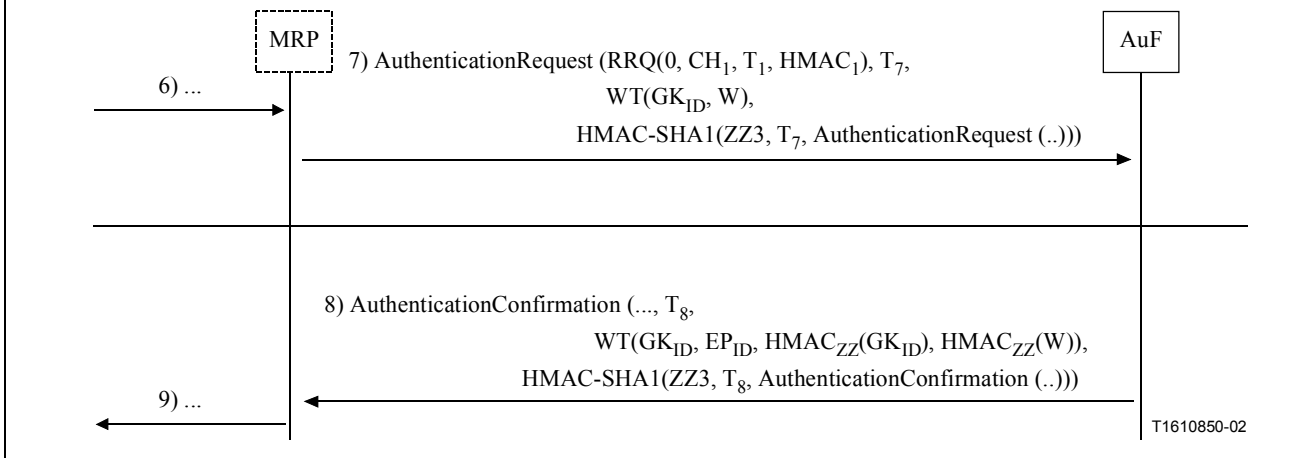


Figure 8/H.530 – Transmission of authentication information between H-BE and MRP

8) Clause 8.2.6

Replace Figure 9:



With:

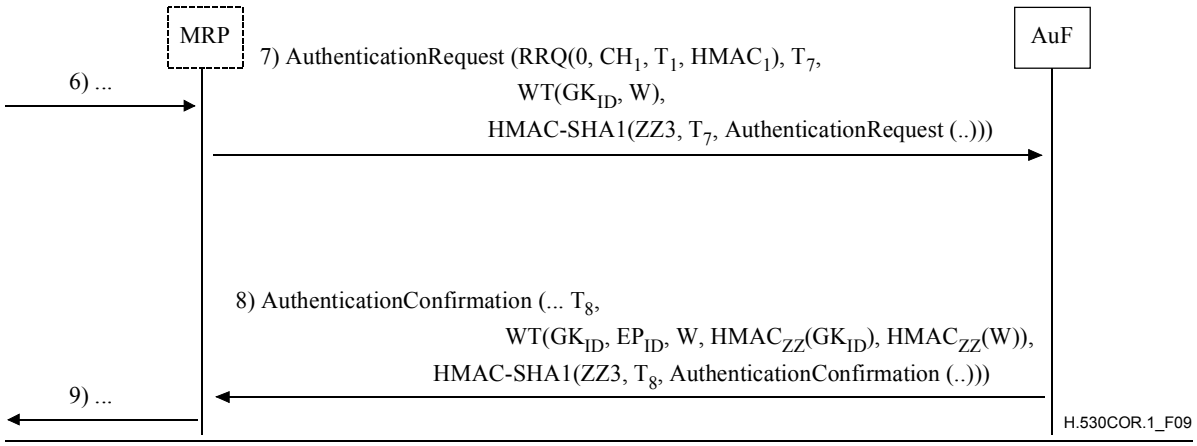


Figure 9/H.530 – Transmission of authentication information between MRP and AuF

9) Clause 8.2.6

Change text as follows:

…

8.2.6 MRP to AuF

…

When the AuF is not able to apply the shared secret *ZZ*, the computation of the authenticated values for the credentials as described below shall be omitted, and no such result shall be included in the **AuthenticationRejection** message. In that case, a mobility **ClearToken** is not present in the **AuthenticationRejection** message.

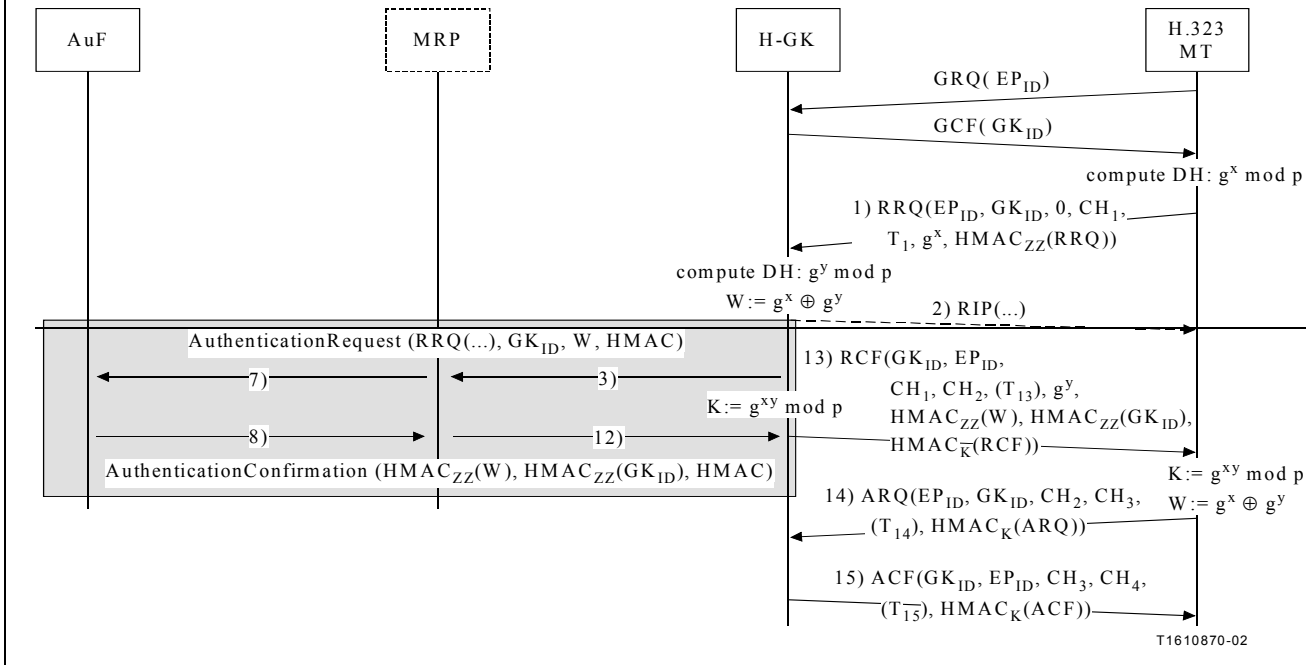
Otherwise, the AuF shall also compute the credentials of the authenticated compound value *W* using HMAC-SHA1-96 key hash function and *ZZ* as the shared key. The authenticated compound value *W* shall be included in a separate mobility **ClearToken**, where the result is stored in the **halfkey** field of the **dhkey** field within that mobility **ClearToken**. Further, the AuF shall compute an authenticated GK_{ID} as another credential using HMAC-SHA1-96 key hash function and *ZZ* as the shared key. The result shall be included within **generator** in that **ClearToken**. The AuF shall also include *W* in the **modsize** field of **dhkey**; this allows the V-GK to recognize **AuthenticationConfirmation**/**AuthenticationRejection** as fresh. The **generalID** shall convey the GK_{ID}, while the **sendersID** shall convey the EP_{ID} in that **ClearToken**. This shall allow the V-GK to associate an **AuthenticationConfirmation**/**AuthenticationRejection** with the corresponding **AuthenticationRequest** message. The **tokenOID** of that **ClearToken** shall be set to "G2" and any other parameters in that mobility **ClearToken** shall be unused. The mobility **ClearToken** is shown as **WT()**.

A new timestamp T_8 shall be used and the response message shall be secured by according to Annex D/H.235 procedure I [4] using the shared secret *ZZ3*; see message 8).

…

10) Clause 8.5

Replace Figure 11:



With:

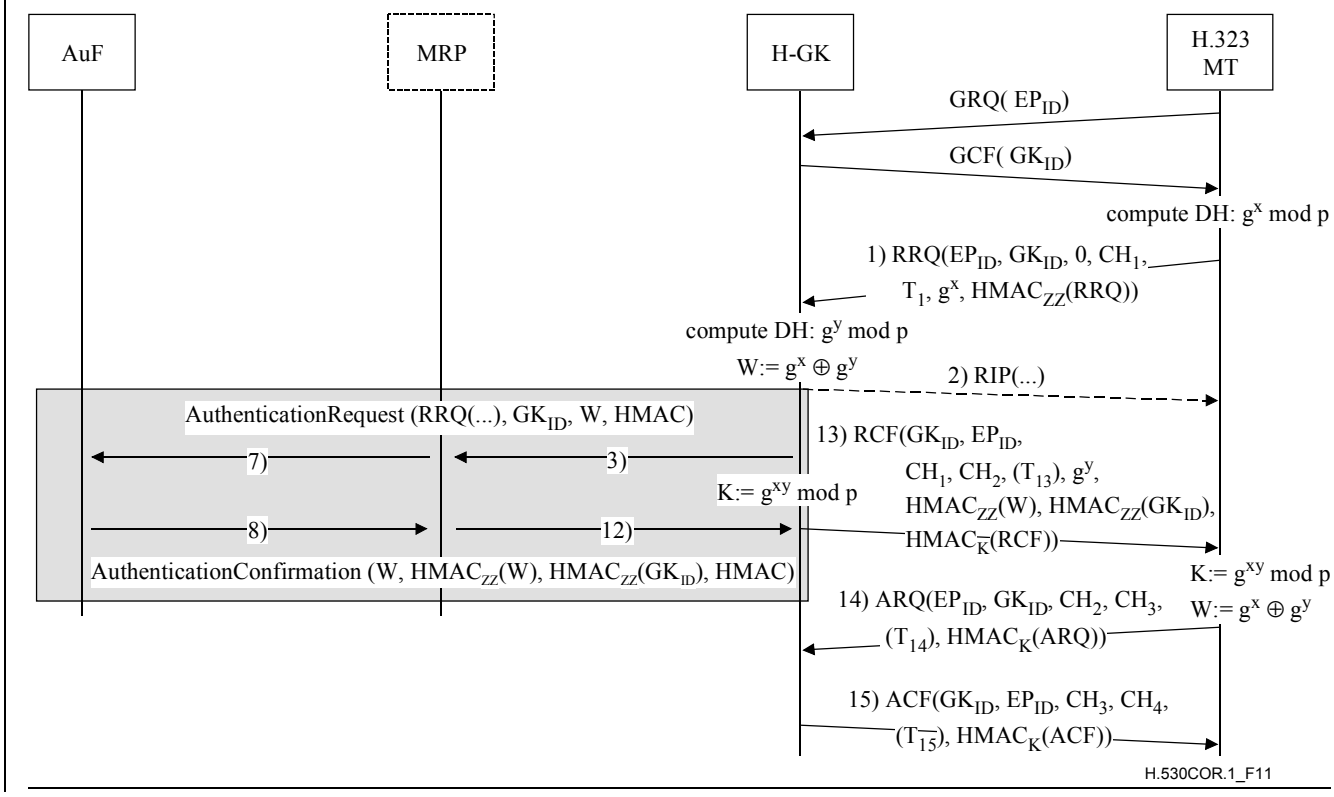


Figure 11/H.530 – MT authentication in the home domain during registration phase

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, 2003