INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.530

(03/2002)

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

ITU-T Recommendation H.530

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.530

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

Summary

The purpose of this Recommendation is to describe security procedures for an H.323 multimedia mobility environment. This Recommendation provides the details about the security procedures for H.510.

Source

ITU-T Recommendation H.530 was prepared by ITU-T Study Group 16 (2001-2004) and approved under the WTSA Resolution 1 procedure on 29 March 2002.

Keywords

Annex D/H.235, authentication, encryption, integrity, key management, mobility, multimedia security, security profile.

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.530

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

1 Scope

The purpose of this Recommendation is to provide recommendations for security procedures in H.323 mobility environments such as under the scope of ITU-T Rec. H.510. This Recommendation provides the details about the security procedures for ITU-T Rec. H.510.

2 Introduction

So far, the signalling capabilities of ITU-T Rec. H.235 in its versions 1 and 2 [4] are designed to handle security in mostly static H.323 [5] environments. Those environments and multimedia systems can achieve some limited mobility within gatekeeper zones; ITU-T Rec. H.323 [5] in general and ITU-T Rec. H.235 [4] specifically provide only very little support for secure roaming of mobile users and terminals across different domains with many involved entities in a mobility, distributed environment for example.

The H.323 mobility scenarios depicted in ITU-T Rec. H.510 [6] regarding terminal mobility pose a new situation with their flexible and dynamic character also from a security point of view. Roaming H.323 users and mobile terminals have to be authenticated by a foreign, visited domain. Likewise, the mobile user would like to obtain evidence about the true identity of the visited domain. In addition to that, it may be also useful to obtain evidence about the identity of the terminals complementing user authentication. Thus, these requirements demand for mutual authentication of the user and the visited domain and optionally also of the identity of the terminal.

As the mobile user is usually known only to the home domain where the user is subscribed and assigned a password, the visited domain initially does not know the mobile user. As such, the visited domain does not share any established security relationship with the mobile user and the mobile terminal. In order to let the visited domain achieve the authentication and authorization assurance for the mobile user and for the mobile terminal, the visited domain would relay certain security tasks such as authorization checks or key management to the home domain through intermediate network and service entities. This requires securing the communication and key management between the visited domain and the home domain too.

While, in principle, mobility H.323 environments are more open than closed H.323 networks, there is of course also need to appropriately secure the key management tasks. It is also true that communication within and across the mobility domains deserves protection against malicious tampering.

In summary, this Recommendation describes a generic security concept for mobility among domains for multimedia applications and multimedia services. The technical details describe the deployment for H.323 and for H.510 in particular, but are considered potentially open to other environments.

3 Specification 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.

References to clauses, subclauses, annexes and appendices refer to those items within this Recommendation unless another Recommendation is explicitly listed. For example, "1.4" refers to clause 1.4 of this Recommendation; "6.4/H.245" refers to clause 6.4 in Recommendation H.245.

This Recommendation shows several mobility functional entities such as border elements. For a general description of those functional elements and their interaction, please refer to ITU-T Rec. H.510 [6]. As this Recommendation only describes user/terminal mobility security, interaction with other mobility related functional entities such as mobility routing proxies like VLF, HLF is just briefly mentioned; such functional entities are considered not an integral part of this Recommendation. Specifically, the security architecture does not depend on the presence or absence of such functional elements nor does the security architecture require separating any such function. For simplicity, this Recommendation rather assumes these functions co-located in compound network elements, but for completeness those network entities are shown as decomposed functional entities. Of course, the security concepts could be extended in a straightforward manner to cover those elements when present as well by functionally decomposing and separating them.

All those optional network entities appear as dashed boxes in the diagrams. Regarding the home domain, an authentication entity (AuF) functioning as a back-end security service may be separate or may be co-located with the home border element or other appropriate H.323 entities [5], e.g. the home gatekeeper (H-GK). Which of those instantiations actually apply is left as a local implementation matter.

In this Recommendation, the **authentication function** (**AuF**) is understood as the security functional entity in the home domain that maintains security relationship with the subscribed mobile users and the subscribed mobile terminals if necessary. Among further tasks not described in this Recommendation, the AuF shall accomplish at least the following tasks:

- Evaluate incoming **AuthenticationRequest** messages from a visited domain, check the authenticity and integrity of such messages, and particularly, the AuF shall authenticate the mobile user and optionally also the mobile terminal (MT) if provided and desired.
- Upon successful authentication of the mobile user/terminal, the AuF shall decide upon granting authorization. Exactly how the AuF would achieve this decision is outside the scope of this Recommendation, but some policy database or certain access rules might be appropriate.
- Further on, the AuF shall support and assist the visited domain in the key management task; specifically, the AuF shall authenticate a received Diffie-Hellman half-key and GK_{ID} from the visited domain using the corresponding user shared secret.
- Finally, the AuF shall respond back to the visited domain about the security authorization decision taken, with the authenticated value Diffie-Hellman half-key and GK_{ID} included.

The AuF could be thought of as a security module – potentially physically separate from other functional entities – with specific security functionality such as protected key storage, cryptographic algorithm and mechanism support, secured administration and maintenance access, reliability, etc. However, this Recommendation does not assume presence of any such feature in the AuF. Rather, the AuF may also well be co-located with other H.323 functional entities [5] in the home domain such as in the border element, in the gatekeeper, in a mobility routing proxy (MRP) or in any other appropriate entity. The concept of the AuF leaves it open on whether it would be best implemented in hardware, in software, or in a combination of both.

This Recommendation introduces a **mobility routing proxy** (**MRP**) as an optional functional entity. The MRP acts as an intermediate functional entity, terminating the security association of a hop-by-hop link. The MRP shall forward the security tokens by re-computing anew the hop-by-hop message authentication codes in the **CryptoToken**. The MRP may encompass the functionality of a mobility management functional entity (e.g. of a HLF or of a VLF or of any other mobility

back-end service entity). The MRP may appear in the visited domain or in the home domain, or in any other domain traversed.

In case a shown MRP does not occur in the actual communication, the hop-by-hop links entering and leaving the MRP shall be considered to belong to the same security association and re-computation of the **CryptoToken** shall be omitted.

This Recommendation uses the term **password** when a user-entered password string is meant. The password in this Recommendation is understood to be the assigned security key, which the mobile user shares with his or her home domain. This user password and derived user shared secret shall be applied for the purpose of user authentication.

Different to that, a **shared secret** is the security key that is part of the security parameters for the cryptographic algorithms; it can be derived from a password (see H.235 procedure 10.3.5 [4]) or it can be assigned per configuration or by other means.

Likewise, the mobile terminal may have been assigned a separate security shared secret by the home domain for the purpose of terminal authentication.

The assignment and distribution of passwords and shared secrets among the functional entities is outside the scope of this Recommendation.

This Recommendation uses the term **service relationship** to reference an established security association between two functional entities, such as between a visited border element (V-BE) and a home border element (H-BE). Among other parameters of such a service relationship, it is essential that at least a shared key *ZZn* be present, by which traffic between both functional entities is secured (e.g. IPSEC or Annex D/H.235 [4]).

The **AuthenticationRejection** message used in this Recommendation indicates a failed security check by the AuF. The **AuthenticationRejection** message shall hold the same **Clear-** and **CryptoTokens** as the related **AuthenticationConfirmation** message.

The object identifiers are referenced through a symbolic reference in the text (e.g. "G1"). Clause 8.6 lists the actual numeric values for the symbolic object identifiers.

4 Terms and definitions

For the purposes of this Recommendation the definitions given in clause 3 of ITU-T Recs H.323 [5], H.225.0 [1], H.225.0 Annex G [2], H.235 [4], H.501 [3], H.510 [6] and X.800 [7] apply along with those in this clause.

4.1 authentication function (AuF): The AuF is the security functional entity in the home domain that maintains security relationship with the subscribed mobile users and the subscribed mobile terminals.

4.2 credential: In this Recommendation, a credential [such as $HMAC_{ZZ}(GK_{ID})$ or $HMAC_{ZZ}(W)$] is understood as some piece of data to which the AuF cryptographically has applied its shared secret *ZZ* that it shares with the mobile user. The credential is transferred to prove authorization and timeliness in the authorization check.

4.3 home border element (H-BE): This is a border element (BE) placed within the home domain.

4.4 mobility routing proxy (MRP): The MRP is an optional functional entity that acts as an intermediate functional entity, terminating the security association of a hop-by-hop link.

4.5 password: Referring to a user-entered password string.

4.6 service relationship: References an established security association between two functional entities, assuming that at least a shared key is present.

4.7 shared secret: Refers to the security key for the cryptographic algorithms; it may be derived from a password.

4.8 visited border element (V-BE): This is a border element (BE) placed within the visited domain.

5 Abbreviations and symbols

This Recommendation uses the following abbreviations and symbols:

AuF	Authentication Function, see ITU-T Rec. H.510 [6]
BE	Border Element, see ITU-T Rec. H.225.0 Annex G [2]
CH_n	Challenge number *n*
DH	Diffie-Hellman
EP_{ID}	MT endpoint identifier, see ITU-T Rec. H.225.0 [1]
GK	Gatekeeper, see ITU-T Rec. H.510 [6]
GK_{ID}	Visited Gatekeeper identifier, see ITU-T Rec. H.225.0 [1]
GRJ	Gatekeeper Reject
GRQ	Gatekeeper Request
H-BE	Home BE
H-GK	Home GK
HLF	Home Location Function
HMAC-SHA1-96	Hashed Message Authentication Code with Secure Hash Algorithm 1
$HMAC_Z$	Key Hashed message authentication code/response with shared secret *Z*, if *Z* is not shown then the next-hop secret is applied
IPSEC	Internet Protocol Security
K	Dynamic session/link key
MRP	Mobility Routing Proxy
MT	Mobile Terminal, see ITU-T Rec. H.510 [6]
NTP	Network Time Protocol
OID	Object Identifier
PKI	Public-key infrastructure
PW	Mobile User Password
R_1	Random number
RIP	Request in Progress
RRJ	Registration Reject
RRQ	Registration Request
SNTP	Simple Network Time Protocol
T_n	Timestamp number *n*
V-BE	Visited BE

V-GK	Visited GK
VLF	Visitor Location Function
W	Compound value with arithmetic combination of Diffie-Hellman half-keys
WT	Mobility ClearToken
XT	CryptoToken for MT authentication
ZZ	Shared secret/password of the mobile user, which is shared with the corresponding AuF
ZZMT	Shared secret of the mobile terminal MT, which is shared with the corresponding AuF
ZZ_n	Shared-secret number *n*
$\oplus$	Bitwise XOR

6 References

6.1 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 below. A list of the currently valid ITU-T Recommendations is regularly published.

[1] ITU-T Recommendation H.225.0 Version 4 (2000), *Call signalling protocols and media stream packetization for packet-based multimedia communications systems*.

[2] ITU-T Recommendation H.225.0 Annex G (Draft), *Communication between administrative domains*.

[3] ITU-T Recommendation H.501 (2002), *Protocol for mobility management and intra/inter-domain communication in multimedia systems*.

[4] ITU-T Recommendation H.235 Version 2 (2000), *Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals*.

[5] ITU-T Recommendation H.323 Version 4 (2000), *Packet-based multimedia communication systems*.

[6] ITU-T Recommendation H.510 (2002), *Mobility for H.323 multimedia systems*.

[7] ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

6.2 Non-normative references

[8] IETF RFC 1305 (1992), *Network Time Protocol (Version 3) Specification, Implementation and Analysis, Internet Engineering Task Force*.

[9] IETF RFC 2030 (1996), *Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI; Internet Engineering Task Force*.

7 Security requirements and constraints for mobility

Multimedia mobility management and application to H.323 mobility environments face the following security requirements and constraints:

- This Recommendation shall support and facilitate better security interworking of H.323-secured systems when deployed in a mobility environment with distributed components and separately managed domains.
- The mobile user shall be authenticated when roaming across domains. The mobile user authentication shall serve as a base for granting user access and service permission. The authentication shall be accomplished through the home AuF when initially attaching to a foreign visited domain. For any further interaction with the visited domain, the mobile user authentication shall be accomplished through the visited domain without necessarily querying the home AuF each time.
- The mobile terminal should be authenticated when roaming across domains. The mobile terminal authentication may be used to detect and trace black-list/white-list MTs. The MT authentication should be accomplished in conjunction with the mobile user authentication, instead of a separate and additional procedure.
- A scenario should be supported where the MTs are maintained in a different AuF (possibly in a different domain) than the mobile users. In such a scenario, the visited domain shall query the user's home domain with a single authentication request rather than separate authentication requests. The user's home AuF may then further delegate queries for the MT authentication, but such communication is not part of this Recommendation.
- Based upon the trust relationship between visited domain and home domain, the visited domain shall authenticate towards the mobile user, e.g. in that the MT is able to authenticate the visited gatekeeper. Likewise, the visited domain should authenticate towards the home AuF.

  NOTE – As visited domain and home domain usually do not share an established security relationship, one cannot expect to achieve strong authentication between those two domains in a strict sense. However, some trust assurance could be achieved by relying on the hop-by-hop secured links between the visited domain and the home domain.
- The mobility management protocols within and across domains shall be secured against masquerade, loss of integrity and if possible against loss of confidentiality.
- Denial-of-service attacks should be minimized as far as possible.
- User profile and user service profile information, as well as any security keys shall be transmitted securely across and within domains. The latter demands secure key management in a mobility environment. This includes the requirement that such sensitive information shall not be made available to any intermediate entities and domains unless required. This means that the MT user password shall not be made available to any functional entity except MT and AuF. This also means that the MT shared secret shall not be made available to any functional entity except MT and AuF. Further, this means that the negotiated dynamic session key for securing communication between the MT and the visited domain shall not be made available to other intermediate network entities.
- The dynamic session key shall be authentic and cryptographically bound to the accomplished authentication. This includes the requirement for the session key to be fresh.
- The overall security architecture shall take the trust relationships among domains into account. On one hand, this requires taking the security relationship among entities and domains into account. On the other hand, cheating entities (such as potentially a masqueraded visited gatekeeper (V-GK) but also any other entity) shall be detected and the likelihood of cheating be minimized.

- The security techniques to be applied shall take existing H.235 [4] and other security techniques into account with enhancement only if necessary.
- The security architecture deployed shall be simple and shall not require assuming additional security infrastructure measures such as smart cards and complex management protocols.

8 Hop-by-hop security with symmetric cryptographic techniques

As symmetric security techniques are deployed according to Annex D/H.235 [4] in non-mobility, quasi-static H.323 environments, this Recommendation shows the security architecture with security procedures in a mobility H.323 environment, which deploys the same security techniques as well. Basically, this Recommendation describes a security architecture that is based upon a security infrastructure only using symmetrically shared secrets. The shared secrets are defined on a hop-by-hop or pair-wise base between the communicating entities.

This is a simple security model and does not require using a specific public-key security infrastructure for example. The hop-by-hop security architecture is designed to deploy well-engineered Annex D/H.235 [4] security symmetric techniques to a large extend. It is believed that symmetric crypto techniques provide rather high performance and thus, such techniques are generally applicable in the mobility environment as well.

Figure 1 depicts the security architecture for an H.323 mobility environment according to H.510 [6], which is based upon H.501 [3]. The figure shows the principal architectural relationship of the functional entities. Furthermore, the figure shows the security relationship of keys among the entities. The figures also shows the case when the MT is attached to home gatekeeper in the home domain.

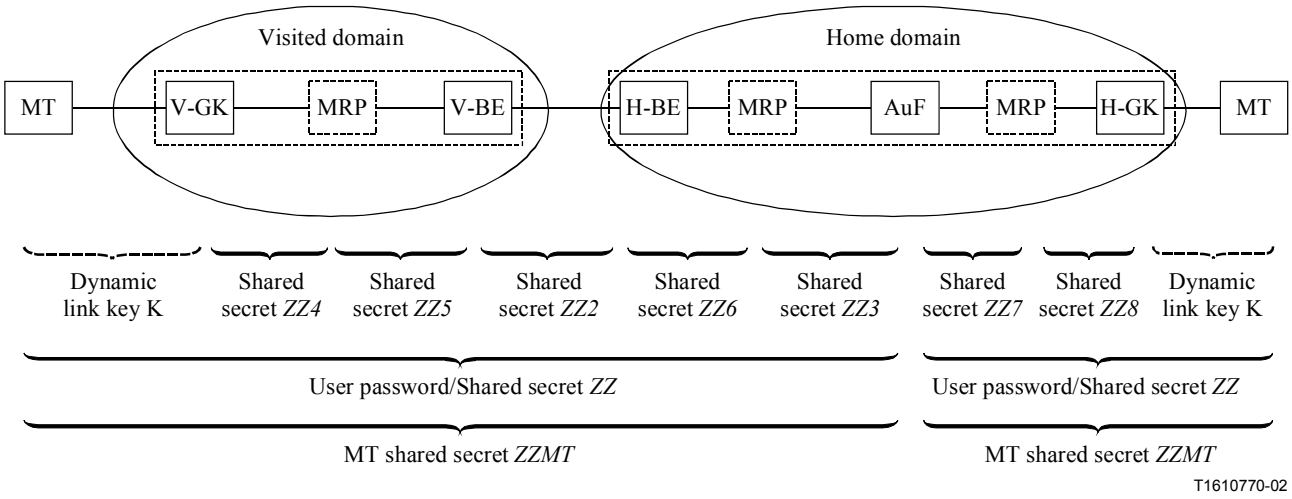

Figure 1/H.530 – Security architecture for mobility H.323 environment

It is assumed that the MT and the AuF in the home domain share an administered password *ZZ* that is assigned during the user's subscription process. Further on, the V-GK and the next functional element one hop away (e.g. a MRP) share a shared secret *ZZ4*, and the MRP shares a shared secret *ZZ5* with V-BE. As an example, if a MRP does not occur in a particular environment, then a shared secret shall be assumed between the V-GK and the V-BE accordingly and the security protection of relayed messages shall be applied accordingly.

It is assumed that the H-BE and a MRP share a shared secret *ZZ6* and the MRP shares a shared secret *ZZ3* with the AuF. Among the domains, there is a shared secret *ZZ2* assumed between V-BE and H-BE or there should be IPSEC or other appropriate network security protection as a generic security means. The shared secrets *ZZ2*-*ZZ6* may be applied for security protection of the H.501 [3] mobility management protocol or may serve as shared secret for underlying IPSEC. While the user

password and the shared secrets *ZZ2*-*ZZ6* and *ZZMT* are statically administered, the link key *K* is dynamically assigned as part of the signalling and authentication procedure. The dynamic link key *K* is shared between the MT and the V-GK.

As described in 8.5, the AuF and the MRP share a shared secret *ZZ7* and the MRP and the H-GK share a shared secret *ZZ8*.

NOTE 1 – This security architecture depends on trusted intermediate nodes. This means that any intermediate nodes such as V-BE and H-BE and potentially also MRP, AuF and GK may read and intercept signalling information in transit that is not actually targeted for them. This should not be a real issue as long as there is full trust assumed within a domain and, further, a tight, mutual trust relationship between visited domain and home domain with no other intermediate domains involved in the H.323 communication [5] in-between these two domains.

NOTE 2 – Generally, using shared secrets limits scalability; thus, only a small number of domains and BE nodes may use this principle in controlled environments. For example, it is anticipated that the security architecture described in this Recommendation scales up to a number of approximately 500 network domains such as proved feasible in the GSM networks. It is assumed that the security architecture herein would not scale well beyond significantly more network domains than those say 500. Thus, support for a large-scale secure mobility environment is left for further study.

8.1 Assumptions

The H.530 security protocol deployed in this Recommendation, when used in conjunction with H.501 [3], assumes synchronized time on each leg in case of Annex D/H.235 [4] techniques applied at the application layer (i.e. V-GK-to-MRP, MRP-to-V-BE, V-BE-to-H-BE, H-BE-to-MRP and MRP-to-AuF). In case of network or transport security techniques applied on those links, synchronized time among the listed entities is not required. The security architecture further assumes synchronized time clocks between the MT and the AuF in the home domain. This could be achieved through NTP (IETF RFC 1305, [8]) or SNTP (IETF RFC 2030, [9]) time and clock synchronization protocols for example.

NOTE – No time synchronization is assumed between the MT and any visited GK. For mutual authentication of the MT and the visited GK, challenge-response security techniques are deployed. No time synchronization is required for IPSEC security protection of H.501 [3].

The H.225.0 RAS [1] protocol shall be applied for signalling communication between MT and V-GK, while the H.501 [3] mobility management protocol shall be applied between any other functional entities shown. H.501 [3] shall use H.235 [4] signalling facilities for message security protection and secured mobility management and may in addition use IPSEC for enhanced security.

8.2 Secure location updating procedures

While the MT and the visited GK usually never had any contact before and thus cannot deploy common subscription information, the visited GK when receiving an initial message from the MT is not able at first to immediately authenticate the MT, and vice versa. For this reason, the V-GK relays the task of MT user authentication and authorization to the AuF in the domain where the MT user is subscribed. The AuF shall perform the user/MT authentication and decide upon the authorization. The AuF responds with the result of the security verification and delivers security information such as credentials towards the visited GK and towards the MT for the session.

Since the authentication and authorization query to the AuF usually only occurs when the MT and the user initially attach to the visited domain, there is no immediate need to execute this procedure at any later point in time during the same call/session, unless explicitly deemed adequate by the V-GK security policy. Thus, the V-GK is able to operate autonomously from the AuF once having received the authorization credentials. This makes the V-GK behave as a local operating security server in the visited domain.

This Recommendation supports two procedures for secure location updating.

Both procedures occur during initial authentication: It is common to both procedures that authentication is identical using **AuthenticationRequest** and **AuthenticationConfirmation** beyond the visited GK. The only difference between the two is that either the **GRQ** or the **RRQ** message is applied.

- Authentication during the V-GK discovery phase: This procedure is applicable when the MT has already an endpoint ID and knows a priori the visited gatekeeper identifier. In this case, it is possible to secure the **GRQ** message according to Annex D; see Figure 2.
- Authentication during the MT and user registration: This procedure applies when the MT does not know the visited gatekeeper identifier and does not yet have an endpoint ID assigned. Thus, MT and GK first complete the discovery procedure (insecure) and thereby exchange their IDs. After that, the MT and user authenticate when sending initial **RRQ**; see Figure 3.

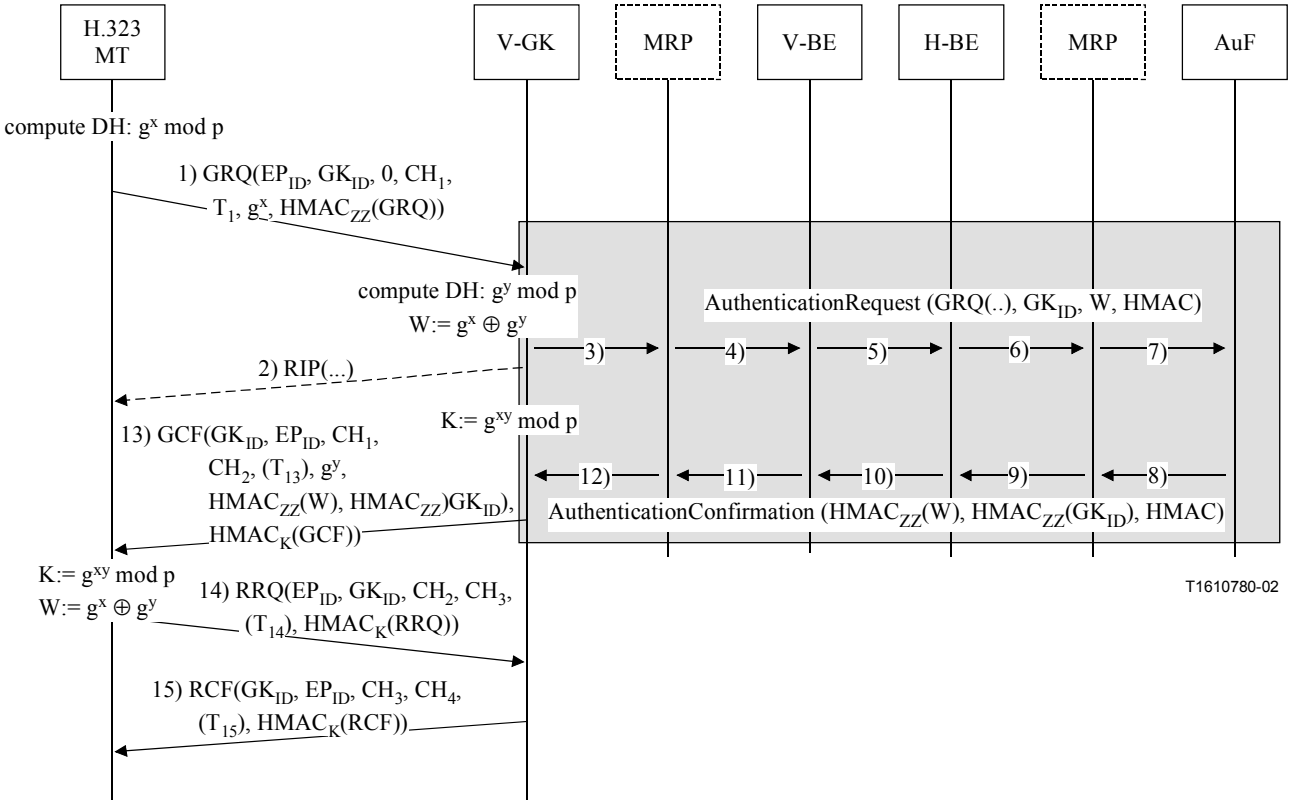

Figure 2/H.530 – Authentication and key management during GK discovery phase

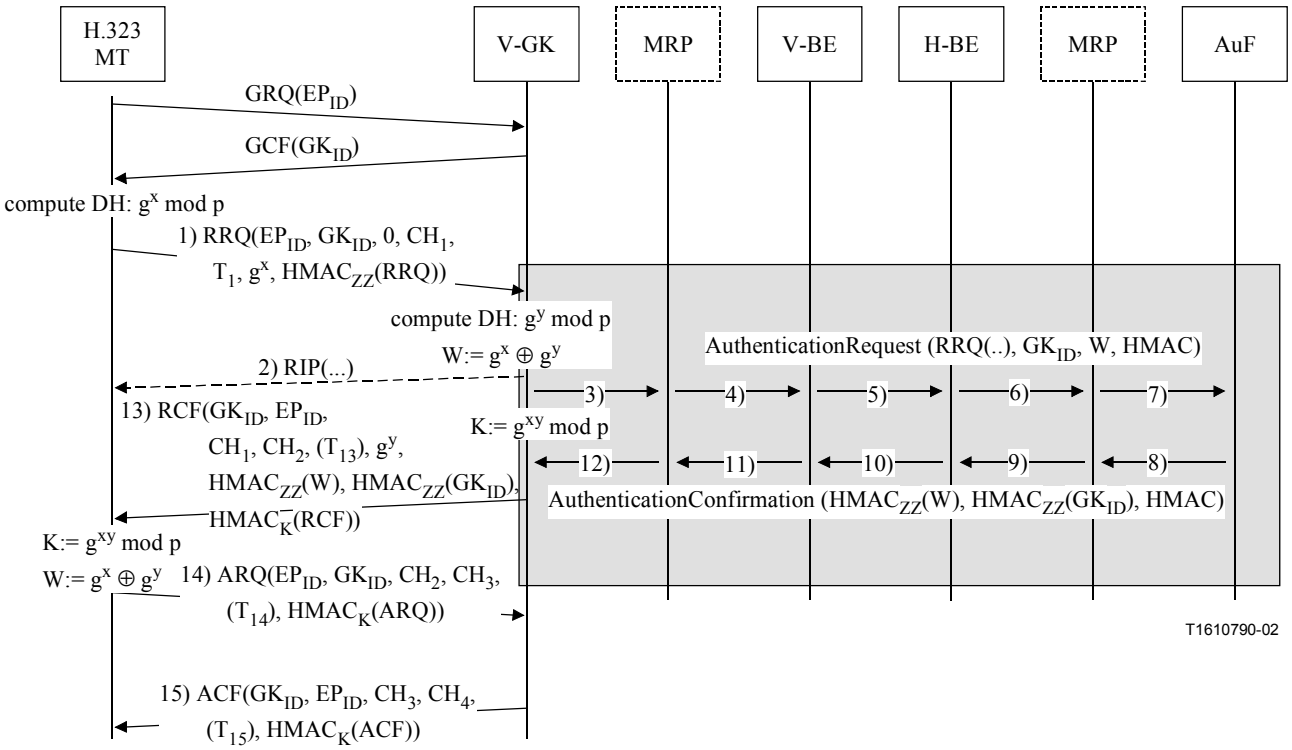

Figure 3/H.530 – Authentication and key management during registration phase

Secure location updating occurs either:

- when a user and an MT contact a visited domain for the first time without any prior information available in the visited domain; or
- when there already is some temporary information available about the MT and the user in the visited domain.

The former case requires full execution of the authentication procedures whereby the visited domain gathers sufficient information from the home domain in order to serve the MT. This procedure includes reporting results of the authentication, authorization check, and credentials by the home domain. This procedure may further carry service profile information towards the visited gatekeeper. It is to be noted that such procedure usually involves network communication and interaction with potentially several entities, and therefore might take some time to complete.

The latter case would not make it necessary for the V-GK to contact the home domain, although this is not precluded. The visited gatekeeper would reuse locally stored information without contacting the home domain. This could happen in case of a lost and re-established connection, or of a local change of the network point of attachment. Whenever the MT possesses a valid link key, the MT shall attempt to use it first before falling back to deploying an initial location update.

Primarily, the user authenticates explicitly by applying the password, which the user obtained at subscription time. However, for mobile terminal authentication, it may optionally also be possible that the MT authenticates additionally towards the AuF (see the procedure described in 8.3).

Basically, the secure location updating procedure proceeds as follows: The initial RAS message that the visited GK receives is encapsulated in an **AuthenticationRequest** and relayed through one or several functional entities to the AuF in the home domain. This is done because the visited GK is not able to authenticate the MT and the user. The AuF verifies the relayed information, authenticates the MT/user and then decides upon the MT/user's authorization using some criterion. Alternatively, the AuF may remember the MT/user and shall deliver result of the authentication and authorization check by credentials towards the V-GK and MT using **AuthenticationConfirmation/ AuthenticationRejection**.

The visited domain authenticates towards the MT/user when delivering the dynamic link key, in response to the challenge of the MT. The MT/user authenticates with any subsequent RAS message towards the V-GK using challenge and response techniques. Likewise, the MT is able to authenticate the V-GK.

Due to the principle of hop-by-hop security, it is necessary for any intermediate nodes or proxies to verify the applied H.235 [4] security on each leg and re-compute the **CryptoToken** with the message digest anew, as long as network or transport security means are not available. If network or transport security means are available, then re-computation of the message digest in the **CryptoToken** may be omitted.

As the execution of the authentication procedures and network communication between V-GK and AuF may take some time, it may be necessary for the V-GK to send a **RIP** message to the MT indicating that the request is in progress.

The diagrams in Figures 4 through 10 depict the message flow and emphasize H.235 [4] security. The depicted message flow is given for the scenario where the authentication occurs during the registration phase. A similar description applies to the procedures when secure location updating occurs during V-GK discovery; in this case, the encapsulated **RRQ** is to be substituted with **GRQ**. The signalling elements for the optional MT authentication are defined in 8.3 and for simplicity they are not shown in most of the figures. For reasons of space and clarity, the message flow is separated into several phases – each in a separate figure – that all belong together. A logical end-to-end message flow results when reading the numbered messages in sequence.

8.2.1 MT to V-GK

Figure 4 shows the initial registration phase between the MT and the visited GK. Each RAS message conveys a new challenge and the previous challenge value. Except for the first message, the HMAC message integrity check value serves as the computed response to the previous challenge; that HMAC shall be computed according to Annex D/H.235 [4] using the dynamic link key *K* as shared secret. The computation of the HMAC shall follow Procedure I of D.6.3.2/H.235 [4]; without using the **timeStamp** field. If the MT or the visited GK include timestamps anyway (such as T_{13}, T_{14} and T_{15}), then these timestamps should not be checked because synchronized time cannot be assumed between MT and V-GK.

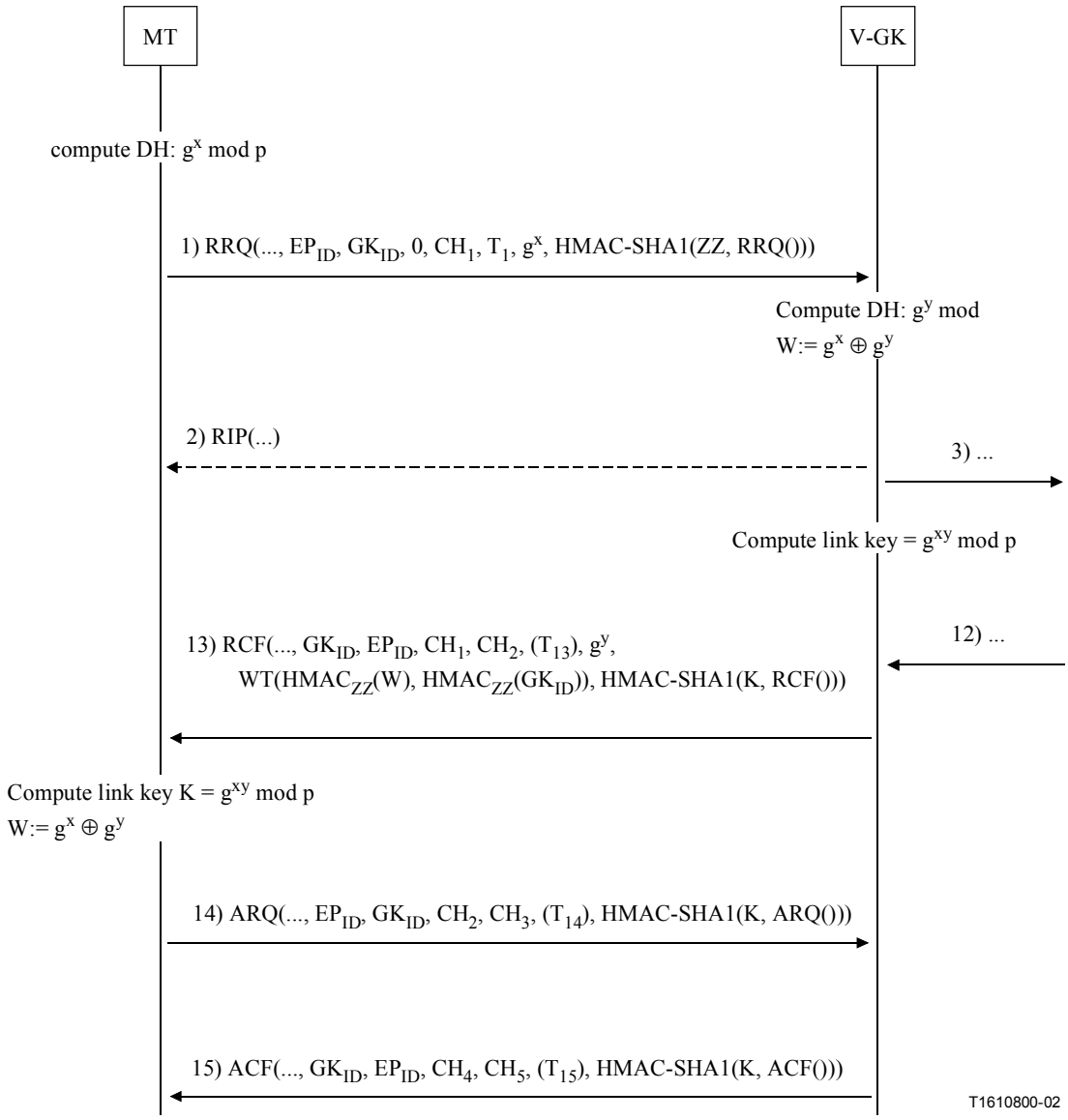

Figure 4/H.530 – Initial registration phase and further RAS messages between MT and V-GK

For the initial registration, the MT shall generate a fresh challenge CH_1 and include it in the **challenge** field in the **ClearToken** of the **RRQ**, see message 1). The **password** field in the **ClearToken** shall convey the previous challenge value. For the initial **RRQ**/**GRQ**, the previous challenge shall be set to all zeros.

Further, the MT shall generate a fresh Diffie-Hellman half-key $g^x \ mod \ p$ with random *x* kept secret and include the half-key in the **halfkey** field of the **dhkey** field within the **ClearToken** of the message. The applied prime number shall be included in **modsize** while the Diffie-Hellman generator shall be included in **generator** of that **ClearToken**. For the Diffie-Hellman (DH) system parameters, the available parameters as given in Table D.4/H.235 [4] shall be taken, where Generator is *2* and the *1024*-bit mod-P prime referred to by "Z" are recommended.

The V-GK receives the challenged **RRQ** and encapsulates it in **applicationMessage** within an **AuthenticationRequest**, see message 3) and sends it to the next hop (e.g. MRP).

The V-GK shall generate a fresh Diffie-Hellman half-key $g^y \ mod \ p$ with random *y* kept secret. For the Diffie-Hellman system parameters, the available parameters as given in Table D.4/H.235 [4] shall be taken; where Generator is *2* and the *1024*-bit mod-P prime referred to by "Z" are recommended.

Taking the received Diffie-Hellman half-key $g^x \ mod \ p$ and its own Diffie-Hellman half-key $g^y \ mod \ p$, the V-GK shall compute a compound value *W* by bitwise XORing both values.

This compound value *W* shall be included in the **halfkey** field of the **dhkey** field within a separate mobility **ClearToken** of the **AuthenticationRequest** message. The **generalID** of that **ClearToken** shall convey the GK_{ID}. The **tokenOID** of that mobility **ClearToken** shall be set to "G2". Any other parameters in that mobility **ClearToken** shall be unused. The AuF will authenticate this **ClearToken** information and compute the corresponding credentials. The mobility **ClearToken** is shown as **WT()**.

The **AuthenticationRequest** message shall convey integrity protection according to Annex D/H.235 [4], unless the link between the V-GK and the next hop (e.g. MRP) is secured by IPSEC.

NOTE 1 – As the mobility **ClearToken** is integral part of the **AuthenticationRequest** message, full message integrity protection already covers the integrity of any conveyed **Clear** and/or **CryptoTokens**. Thus, no separate protection of the mobility **ClearToken** is necessary.

The V-GK may submit an unsecured **RIP** message to the MT to indicate message processing in progress, see message 2). Due to the fact that the MT and visited GK do not share a common secret yet, the V-GK is not able to authenticate and integrity protect this immediate **RIP** message.

NOTE 2 – The MT should not trust unprotected **RIP** messages as they might not be authentic, they might be replayed or stem from denial-of-service attacks. The MT should be prepared to treat replayed **RIP** messages and cope with potential message flooding. It is up to the security policy of the MT how to treat such unprotected **RIP** messages.

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 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 **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).

In addition to the authorization check performed by the AuF, the visited GK may decide by its own criteria on whether to allow or disallow the MT. Thus, the visited GK may reject a **GRQ**/**RRQ** even if the AuF confirmed authentication and authorization. In such a case, the visited GK shall respond with a **GRJ**/**RRJ** indicating the **reason** according to B.2.2/H.235 [4].

The MT receives the protected **RCF** with challenges, Diffie-Hellman half-key and credentials such as the authenticated compound value *W* and authenticated GK_{ID}; see message 13). The MT extracts these parameters from the mobility **ClearToken**. The MT shall compute the dynamic link key *K* in an analogue fashion as the V-GK did and as described above. The MT shall verify the HMAC as response of the entire **RCF** message using the link key *K*. The MT shall compute the compound value *W* by bitwise XORing the received $g^y \ mod \ p$ and its own $g^x \ mod \ p$. The MT shall verify the correctness of the authenticated compound value *W* in the **halfkey** field in the mobility **ClearToken** by applying the shared secret *ZZ*. The MT shall verify the correctness of the authenticated GK_{ID} in the **generator** field in the mobility **ClearToken** by applying the shared secret *ZZ*. If the authenticity of either value cannot be proved, the link key *K* or the V-GK cannot be assumed to be authentic either. This may indicate fraudulent network entities or failed authentication in general. In this case, the MT shall ignore the **RCF** and restart again with a fresh **RRQ**.

In case the V-GK receives an **AuthenticationRejection** and indicated **reason**, then the V-GK shall send an **RRJ** to the MT, see message 13). The security **reason** indicates a security error, as the AuF probably was not able to identify the MT/user. The V-GK shall then forward this error in **RRJ reason**.

As MT and V-GK do not share synchronized clocks, any optional timestamps conveyed within a RAS message shall be ignored.

NOTE 3 – Since the V-GK cannot authenticate an initial unprotected **GRQ**/**RRQ** message, they might be replayed or stem from denial-of-service attacks. Visited gatekeepers receiving an unexpectedly high number of protected or unprotected RAS messages may assume a denial-of-service attack and immediately refuse further message processing.

8.2.2 V-GK to MRP

The communication between the V-GK and the next hop functional element (e.g. MRP) serves the following purposes:

- relaying authentication and authorization of the MT and user towards the AuF;
- relaying authorization confirmation from the AuF towards the MT.

Figure 5 shows the protocol message flow. The **AuthenticationRequest** message 2) entirely carries the RRQ/GRQ RAS message as received from the MT. Further, the **AuthenticationRequest** message carries a mobility **ClearToken** conveying compound value *W* and the GK_{ID}. The mobility **ClearToken** is shown as **WT()**. If authentication of the MT is performed, the V-GK includes a separate **CryptoToken** for that purpose; see 8.3.

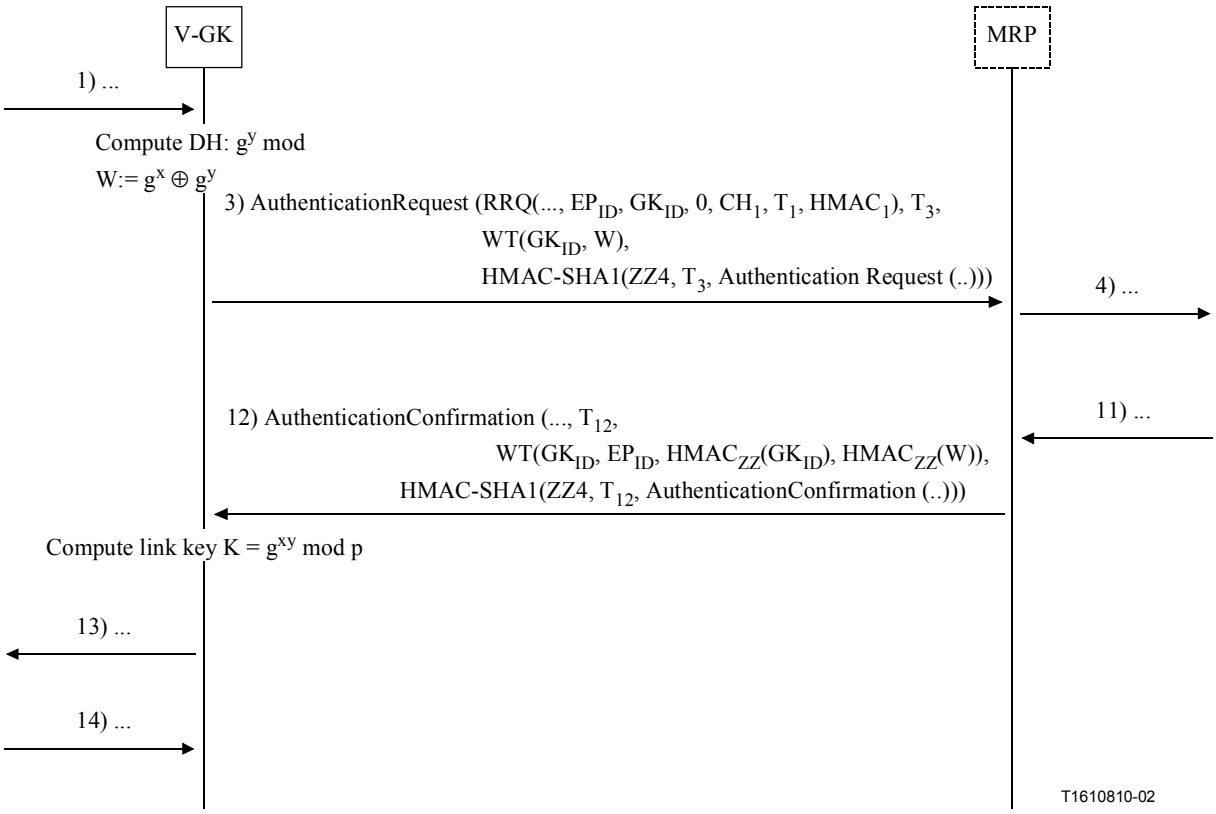

Figure 5/H.530 – Transmission of authentication information between V-GK and MRP

In case the link between V-GK and MRP is not protected by network security (e.g. IPSEC), **AuthenticationRequest** shall be secured according to Annex D/H.235 [4] with a new timestamp T_3 and HMAC computed with key *ZZ4*. Otherwise, **AuthenticationRequest** message may not need security protection by Annex D/H.235 [4].

AuthenticationConfirmation or **AuthenticationRejection** in message 12) carry the authenticated values from the AuF as credentials in a separate mobility **ClearToken** shown as **WT()**. If the link between V-GK and MRP is not protected by network security (e.g. IPSEC), **AuthenticationConfirmation** shall be secured according to Annex D/H.235 [4] with a new timestamp T_{12} and HMAC with key *ZZ4*. Otherwise, **AuthenticationConfirmation/ AuthenticationRejection** may not need security protection by Annex D/H.235 [4].

The conveyed GK_{ID} and EP_{ID} within that mobility **ClearToken** allow the V-GK to associate the received **AuthenticationConfirmation**/**AuthenticationRejection** message with the corresponding **AuthenticationRequest** message.

In case the V-GK does not have a service relationship with the MRP (e.g. missing key *ZZ4*), then the V-GK shall not send an **AuthenticationRequest** but rather respond with **AuthenticationRejection** and **reason** set to **noServiceRelationship**.

8.2.3 MRP to V-BE

A MRP (if present and the conveyed hop count is not exceeded and if a service relationship is present with the V-BE) shall forward the received **AuthenticationRequest** message to the V-BE; see message 4) in Figure 6. The forwarded message shall be secured according to Annex D/H.235 [4] with a new timestamp T_4 and HMAC computed with key *ZZ5*. Otherwise, **AuthenticationRequest** message may not need security protection by Annex D/H.235 [4].

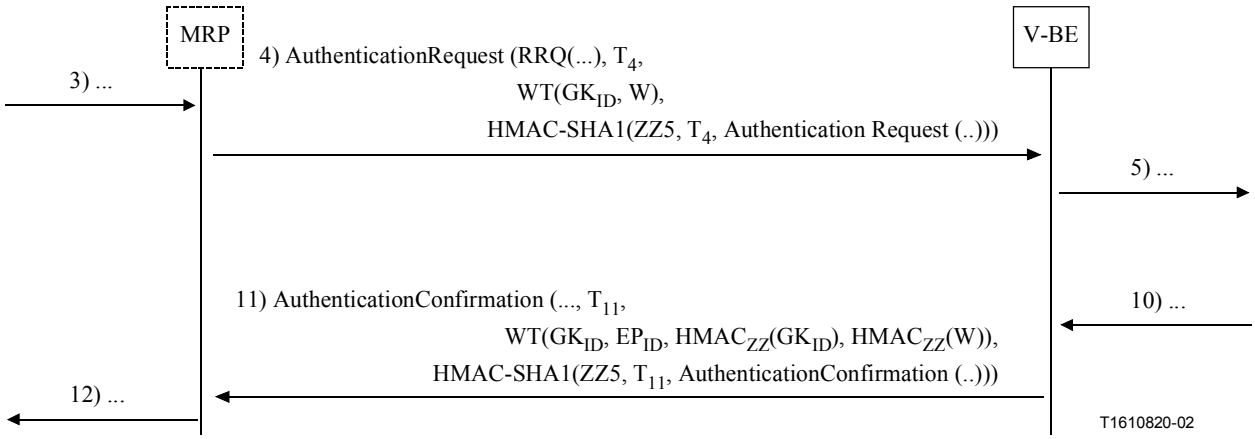

Figure 6/H.530 – Transmission of authentication information between MRP and V-BE

A V-BE shall forward an **AuthenticationConfirmation** or an **AuthenticationRejection** to the MRP.

AuthenticationConfirmation or **AuthenticationRejection** in message 11) carry the authenticated values as credentials from the AuF. If the link between V-BE and MRP is not protected by network security (e.g. IPSEC), **AuthenticationConfirmation/AuthenticationRejection** shall be secured according to Annex D/H.235 [4] with a new timestamp T_{11} and HMAC with key *ZZ5*. Otherwise, **AuthenticationConfirmation/AuthenticationRejection** may not need security protection by Annex D/H.235 [4].

If the hop count is exceeded, then the MRP shall not send an **AuthenticationRequest** message, but it shall rather reply with the **AuthenticationRejection** with reason set to **hopCountExceeded**; (see message 12).

In case the MRP does not have a service relationship with the V-BE (e.g. missing key *ZZ5*), then the V-GK shall not send an **AuthenticationRequest**, but it shall rather respond with **AuthenticationRejection** and **reason** set to **noServiceRelationship**; see message 12).

8.2.4 V-BE to H-BE

Figure 7 depicts the message flow between two BEs of two adjacent domains at the time of initial registration. Security may be realized either using IPSEC according to ITU-T Rec. H.501 [3] or by using the shared secret *ZZ2* that is shared between V-BE and H-BE. In the latter case, the H.501 [3] message shall be secured according to Annex D/H.235 [4].

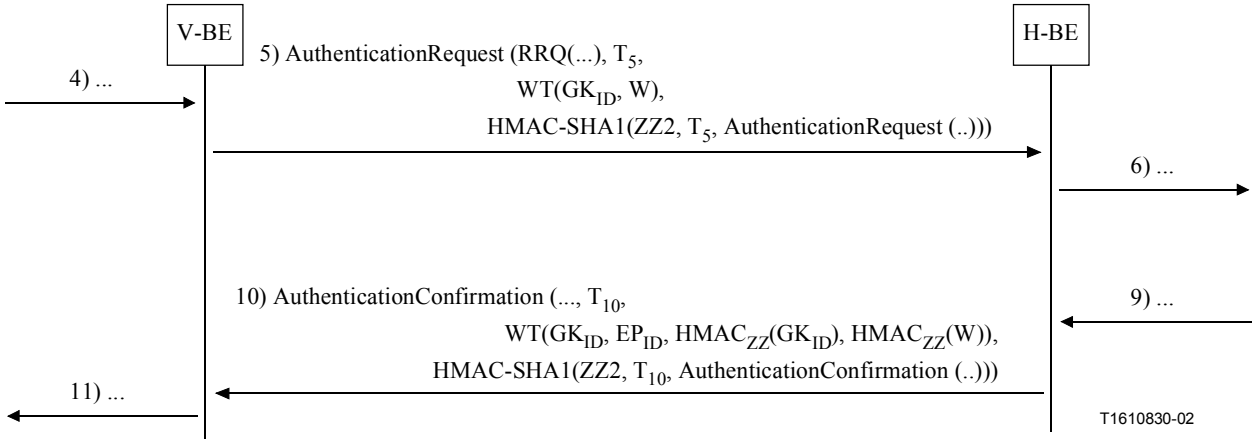

Figure 7/H.530 – Transmission of authentication information between BEs

If the conveyed hop count is not exceeded and a service relationship is present with the H-BE, the H.501 [3] **AuthenticationRequest** message carries the entire **RRQ** including the related Clear- and CryptoTokens; see message 5). This is done to let the AuF validate the **RRQ** message and authenticate the user/MT. An H.501 [3] message is secured such that the entire message is integrity-protected similarly as described by Annex D/H.235, where the computed hash is stored in the **CryptoToken** of the **MessageCommonInfo**. BEs shall insert new timestamps (T_5, T_{10}) for each H.501 [3] message.

The **AuthenticationConfirmation/AuthenticationRejection** carry the authenticated values as credentials from the AuF in a mobility **ClearToken** shown as **WT()**.

In case the MT user is not authorized to use the mobile H.323 service, the AuF should send **AuthenticationRejection** with **reason** set to security. For any other security failure, the AuF shall set **reason** to an error as appropriate to B.2.2/H.235 [4].

If the hop count is exceeded, then the V-BE shall not send an **AuthenticationRequest** message, but rather reply with the **AuthenticationRejection** with reason set to **hopCountExceeded**; see message 11).

In case the V-BE does not have a service relationship with the H-BE (e.g. missing key *ZZ2*), then the V-BE shall not send an **AuthenticationRequest**, but rather respond with **AuthenticationRejection** and **reason** set to **noServiceRelationship**; see message 11).

8.2.5 H-BE to MRP

In case a MRP is present, the message flow proceeds according to Figure 8.

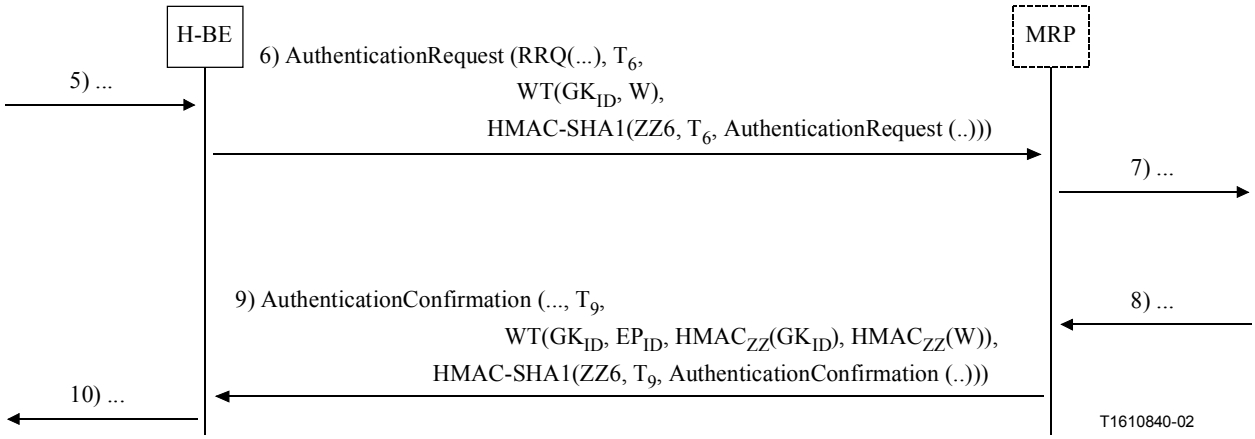

Figure 8/H.530 – Transmission of authentication information between H-BE and MRP

8.2.6 MRP to AuF

Figure 9 shows the message flow between the MRP (if present, if the hop count is not exceeded and if a service relationship is present) and the AuF. If no MRP is present, then the previous network entity shall be substituted instead. Similar to the figures before, the shared secret *ZZ3* secures the transmitted messages.

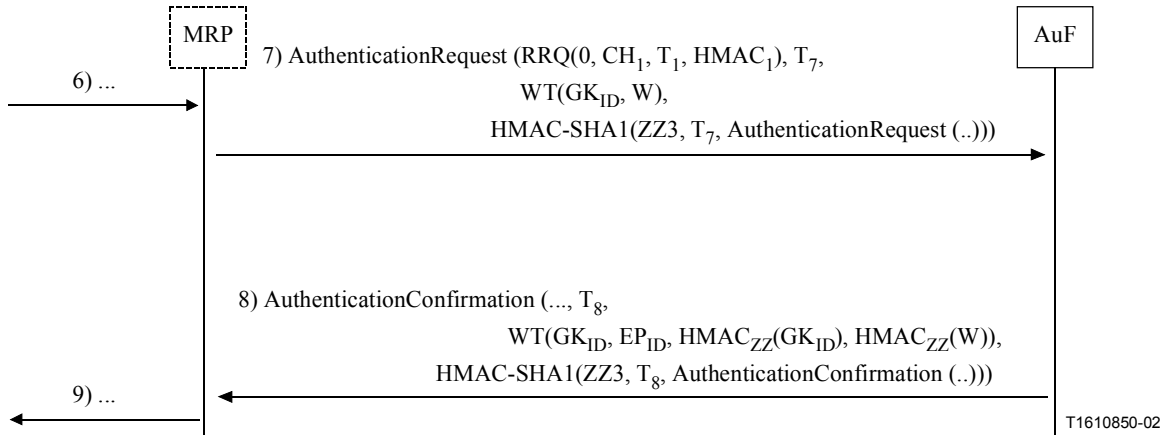

Figure 9/H.530 – Transmission of authentication information between MRP and AuF

Upon reception of the **AuthenticationRequest**, the AuF may successively trust the other functional entities in the chain to have preserved the integrity of the conveyed **RRQ**; see message 7). The AuF shall verify the **AuthenticationRequest** and then verify the encapsulated **RRQ** as described by Annex D/H.235 procedure I [4]. The conveyed timestamp T_1 indicates freshness of the **RRQ** and shall be checked.

If the MT/user is known to the AuF and authorized, the AuF shall respond with **AuthenticationConfirmation**; see message 8). Further, if MT authentication is desired, the AuF shall verify the corresponding conveyed **CryptoToken**. Otherwise, when the MT/user cannot be authenticated or is unknown to the AuF, a protected **AuthenticationRejection** shall be submitted with a **reason** set to an appropriate error as defined in B.2.2/H.235 [4].

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 **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).

If the hop count is exceeded, then the MRP shall not send an **AuthenticationRequest** message, but rather reply with the **AuthenticationRejection** with reason set to **hopCountExceeded**; see message 9).

If the MRP does not have a service relationship with the AuF (e.g. missing key *ZZ3*), then the MRP shall not send an **AuthenticationRequest**, but rather respond with **AuthenticationRejection** and **reason** set to **noServiceRelationship**; see message 9).

NOTE – The AuF is not able to fully authenticate the V-GK in a strict sense. This is because the V-GK is not able to cryptographically prove its identity. However, the AuF certifies by the credential whatever V-GK identity is submitted. Thus, the MT/user is assured that the V-GK with which the MT/user is talking is always the same one as has been certified during the authentication procedure.

8.3 Terminal authentication

Authentication of the mobile terminal (MT) is an additional, optional feature, which is supported in addition to authentication of the mobile user. MT authentication shall be used, when mobile user authentication alone is not considered sufficient and when the MT has a corresponding shared secret *ZZMT*. It is assumed that the mobile terminal owns an assigned shared secret *ZZMT*, which it shares with the AuF. Assignment and distribution of this shared secret is outside the scope of this Recommendation.

Actually, two scenarios for MT authentication are supported:

- The AuF to which the mobile user is subscribed is identical to the AuF that maintains the subscribed MTs. In this case, the AuF is able to authenticate and decide upon authorization both for the user and the MT.
- The AuF to which the mobile user is subscribed is different from the AuF where the MT is subscribed. In this case, the **AuthenticationRequest** shall first be sent to the user's AuF. It is the responsibility of that user AuF to locate and contact the appropriate MT AuF that is responsible for the MT. Such an MT AuF may be located in a different domain. Any such communication and necessary security protection beyond the AuF or among AuFs are outside the scope of this Recommendation.

Authentication of the mobile terminal is accomplished in conjunction with user authentication. For terminal authentication, a separate **CryptoToken** XT() is used. This **CryptoToken** is carried within the security fields of the user authentication messages of either **GRQ** or **RRQ**, depending on whether user and terminal authentication occurs during the discovery phase of the visited GK or during the registration phase; see 8.2.

The mobile terminal authenticates itself towards the AuF by proving knowledge or possession of the shared secret *ZZMT*. This allows the AuF to verify correctness the provided **CryptoToken** and to acknowledge this property as part of the authorization response (**AuthenticationConfirmation**/ **AuthenticationRejection**) back to the visited domain. Then, the visited domain can decide upon the authorization of the MT.

The keyed HMAC-SHA1-96 algorithm is used as the cryptographic authentication function. The procedure deployed basically follows the procedure I of Annex D/H.235 [4] with the exception that the integrity check is computed just over the specific mobile terminal **CryptoToken**, instead of over the entire message as actually described by Annex D/H.235 procedure I [4].

The specific **CryptoH323Token** for mobile terminal authentication shall contain the following fields:

- **NestedCryptoToken** containing a **CryptoToken**, which itself contains the **cryptoHashedToken** containing the following fields:
  - **TokenOID** set to:
    - "G1" indicating the authentication/integrity computation includes only the contents of this **CryptoToken**.
- **HashedVals** containing the **ClearToken** field used with the following fields:
  - **TokenOID** set to:
    - "T" indicating that **ClearToken** is being used for authentication/integrity (see D.11/H.235 [4]).

- **timestamp** containing the time stamp.
- **random** containing a monotonically increasing sequence number. This number allows to make unique two messages with the same timestamp (within the clock resolution).
- **generalID** containing the identifier of the recipient (only in case of unicast messages). In this scenario, this is the identifier of the home domain.
- **sendersID** contains the identifier of the sender. In this scenario, this is the endpoint identifier of the MT.

• **Token** containing **HASHED** with the fields:

- **algorithmOID** set to "U" indicating HMAC-SHA1-96; (see D.11/H.235 [4]).
- **params** set to NULL.
- **hash** containing the authenticator computed using HMAC-SHA1-96. The authenticator shall be computed over the entire **CryptoH323Token**.

The receiving AuF shall verify the found **CryptoToken**, which is conveying MT authentication. In case the verification check fails, the AuF shall consider the MT not as authorized. In this case, the AuF shall respond with **AuthenticationRejection** and reason set to **security**. For any other security failure, the AuF shall set **reason** to an error according to B.2.2/H.235 [4].

Figure 10 shows the message flow for mobile terminal authentication during the registration phase of the mobile terminal. The specific **CryptoToken** for MT authentication is shown as XT().

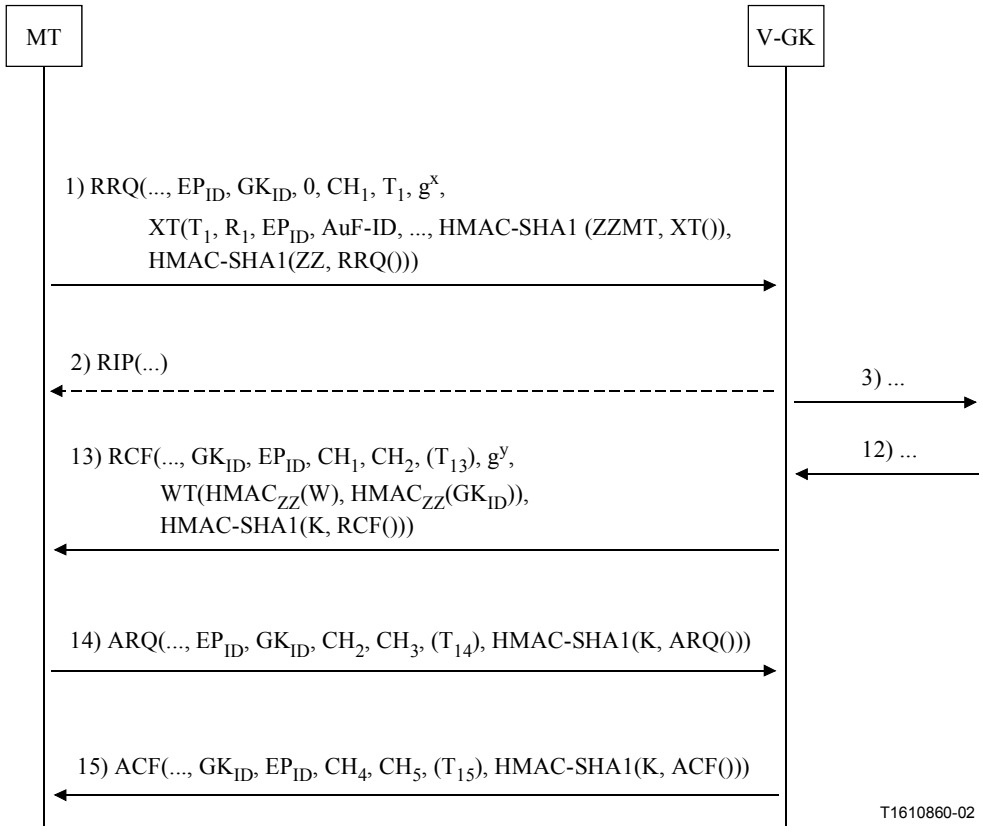

Figure 10/H.530 – MT authentication

The authentication procedure of the MT shall be done explicitly only during **GRQ** or **RRQ**. In any later RAS messages exchanged between the MT and the V-GK, MT authentication is done implicitly through the ongoing user authentication and message integrity. No particular means for further MT authentication are necessary.

8.4 Unregistration

A MT or V-GK upon reception of **UCF** shall release the link key *K*.

8.5 Application of the symmetric security protocol in the home domain

While the security mobility protocol described in this Recommendation would usually be deployed for MTs attached to foreign visited domains, this clause describes the case how this security mobility protocol may also be deployed for MTs attached to the home domain. This allows deployment of the mobility security protocol to be independent of where the MT actually attaches. It includes the case also for non-mobility environments, which nevertheless supports H.530.

Figure 11 shows the scenario where an MT is attached to the home GK in the home domain and the authentication and authorization occurs during the registration phase. A similar scenario not shown is also possible, where the authentication and authorization occur during the gatekeeper discovery phase.

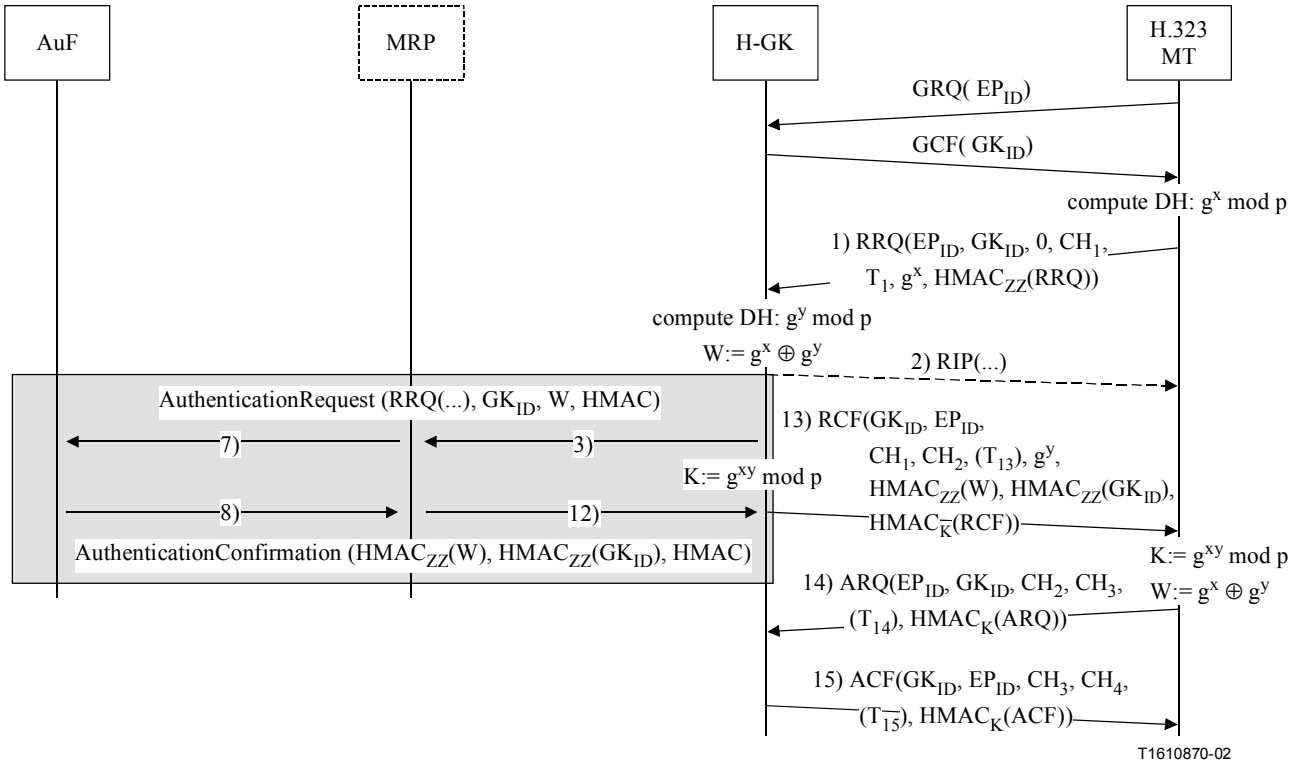

Figure 11/H.530 – MT authentication in the home domain during registration phase

In any case, the H-GK shall behave exactly as a V-GK in the visited domain as shown in Figure 11 and following the security procedures respectively as described above. The shared secret *ZZ4* shall be substituted by *ZZ8*, and *ZZ3* by *ZZ7*, respectively.

The MRP shown is an optional entity. When the MRP is not present, AuF and H-GK have a direct security relationship established. As a special case, AuF and H-GK may even be co-located, thus making communication between both entities a local issue.

8.6 List of Object Identifiers

Table 1 lists all the OIDs referenced in this Recommendation.

Table 1/H.530 – Object Identifiers used by H.530

Object Identifier reference	Object Identifier value(s)	Description
"G1"	{itu-t (0) Recommendation (0) h (8) 235 version (0) 2 10}	Used to indicate a mobility **CryptoToken** for authentication of the MT
"G2"	{itu-t (0) Recommendation (0) h (8) 235 version (0) 2 11}	Used to indicate a mobility **ClearToken** that holds GK_{ID} and compound value *W* within **AuthenticationRequest** or the corresponding AuF-authenticated values within **AuthenticationConfirmation**/ **AuthenticationRejection** or GCF/GRJ, RCF/RCF

9 End-to-end security

An end-to-end security architecture in an H.323 mobility environment that is relying on a public-key infrastructure (PKI) concepts is subject of further study.

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

Printed in Switzerland
Geneva, 2002