



TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(03/2002)

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.

© ITU 2002

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Scope	1
2	Introduction	1
3	Specification conventions	1
4	Terms and definitions	3
5	Abbreviations and symbols	4
6	References	5
6.1	Normative references	5
6.2	Non-normative references	5
7	Security requirements and constraints for mobility	6
8	Hop-by-hop security with symmetric cryptographic techniques	7
8.1	Assumptions	8
8.2	Secure location updating procedures	8
8.2.1	MT to V-GK	11
8.2.2	V-GK to MRP	14
8.2.3	MRP to V-BE	15
8.2.4	V-BE to H-BE	16
8.2.5	H-BE to MRP	17
8.2.6	MRP to AuF	17
8.3	Terminal authentication	19
8.4	Unregistration	21
8.5	Application of the symmetric security protocol in the home domain	21
8.6	List of Object Identifiers	22
9	End-to-end security	22

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 ZZ_n 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.