

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.235.4

(09/2005)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS
Infrastructure of audiovisual services – Systems aspects

H.323 security: Direct and selective routed call security

ITU-T Recommendation H.235.4

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.349
Directory services architecture for audiovisual and multimedia services	H.350–H.359
Quality of service architecture for audiovisual and multimedia services	H.360–H.369
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 H.235.4 2005

ITU-T Recommendation H.235.4

H.323 security: Direct and selective routed call security

Summary

The purpose of this Recommendation is to provide recommendations of security procedures for using direct-routed call signalling in conjunction with H.235.1 and H.235.3 security profiles. This security profile is offered as an option and may complement the security profiles in ITU-T Recs H.235.1 and H.235.3. It also provides implementation details for clause 8.4/H.235.0 using symmetric key management techniques.

In earlier versions of the H.235 subseries, this profile was contained in Annex I/H.235. Appendices IV, V, VI to H.235.0 show the complete clause, figure, and table mapping between H.235 versions 3 and 4.

Source

ITU-T Recommendation H.235.4 was approved on 13 September 2005 by ITU-T Study Group 16 (2005-2008) under the ITU-T Recommendation A.8 procedure.

Keywords

Authentication, direct-routed call security, encryption, integrity, key management, multimedia security, security profile, selective routed call security.

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 not 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 2006

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	References.....	1
2.1	Normative references.....	1
2.2	Informative references.....	1
3	Terms and definitions	2
4	Symbols and abbreviations	2
5	Conventions	2
6	Introduction	2
7	Overview	3
8	Limitations.....	4
9	Procedure DRC1 (corporate environment).....	4
9.1	GRQ/RRQ phase	4
9.2	ARQ phase.....	4
9.3	LRQ phase	4
9.4	LCF phase.....	5
9.5	ACF phase	6
9.6	SETUP phase.....	7
10	Procedure DRC2 (interdomain environment).....	9
10.1	GRQ/RRQ phase	9
10.2	ARQ phase.....	9
10.3	LRQ phase	9
10.4	LCF phase.....	9
10.5	ACF phase	10
10.6	SETUP phase.....	12
11	Procedure DRC3 (interdomain environment).....	14
11.1	GRQ/RRQ phase	14
11.2	ARQ phase.....	14
11.3	LRQ phase	14
11.4	LCF phase.....	14
11.5	ACF phase	15
11.6	SETUP phase.....	16
12	PRF-based key derivation procedure.....	18
13	FIPS-140-based key derivation procedure.....	18
14	List of object identifiers.....	19



Documents

Document Sharing Hub

ITU-T Rec. H.235.4 (09/2005)

iii

ITU-T Recommendation H.235.4

H.323 security: Direct and selective routed call security

1 Scope

The purpose of this Recommendation is to provide recommendations of security procedures for using direct-routed and selective routed call signalling in conjunction with H.235.1 and H.235.3 security profiles.

This security profile is offered as an option and may complement the H.235.1 or H.235.3 security profiles. It also provides implementation details for clause 8.4/H.235.0 using symmetric key management techniques.

2 References

2.1 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. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- ITU-T Recommendation H.225.0 (2003), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.
- ITU-T Recommendation H.235 (2003), *Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals*, Corrigendum 1 (2005), plus Erratum 1 (2005).
- ITU-T Recommendation H.235.0 (2005), *H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems*.
- ITU-T Recommendation H.235.1 (2005), *H.323 security: Baseline security profile*.
- ITU-T Recommendation H.235.3 (2005), *H.323 security: Hybrid security profile*.
- ITU-T Recommendation H.235.6 (2005), *H.323 security: Voice encryption profile with native H.235/H.245 key management*.
- ITU-T Recommendation H.323 (2003), *Packet-based multimedia communications systems*.
- ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
- ISO/IEC 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference model – Part 2: Security Architecture*.
- ISO/IEC 10118-3:2004, *Information technology – Security techniques – Hash functions – Part 3: Dedicated hash-functions*.

2.2 Informative references

- ITU-T Recommendation H.235.2 (2005), *H.323 security: Signature security profile*.
- IETF RFC 4120 (2005), *The Kerberos Network Authentication Service (V5)*.

3 Terms and definitions

For the purposes of this Recommendation the definitions given in clause 3 of ITU-T Recs H.323, H.225.0, H.235.0 and X.800 | ISO 7498-2 apply.

4 Symbols and abbreviations

This Recommendation uses the following abbreviations:

CT	ClearToken
DH	Diffie-Hellman
DRC	Direct-Routed Call
EK_{AG}	The encryption key shared between EP A and GK G
EK_{BH}	The encryption key shared between EP B and GK H
EK_{GH}	The encryption key shared between GK G and GK H
$ENC_{K; S, IV}(M)$	EOFB Encryption of M using secret key K and secret salting key S and initial vector IV
EPID	Endpoint Identifier
GK	Gatekeeper
GKID	Gatekeeper Identifier
g^x, g^y	Diffie-Hellman half-key of GK G, GK H
K_{AB}	The encryption key shared between EP A and EP B
K_{AG}	Shared secret (H.235.1, H.235.3) between EP A and GK G
K_{BH}	Shared secret (H.235.1, H.235.3) between EP B and GK H
K_{GH}	Secret, secret (H.235.1, H.235.3) between GK G and GK H
KS_{AG}	Secret, shared salting key between EP A and GK G
KS_{BH}	Secret, shared salting key between EP B and GK H
KS_{GH}	Secret, shared salting key between GK G and GK H
PRF	Pseudo-Random Function

5 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.

The object identifiers are referenced through a symbolic reference in the text (e.g., "I11"), clause 14 lists the actual numeric values for the symbolic object identifiers, see also clause 5/H.235.0.

6 Introduction

H.323 is often deployed using the gatekeeper-routed model (for example, to take advantage of better billing functionalities). The widespread use of gatekeeper-routed call models is also the

reason why different security profiles, focused exactly on this call model, are defined within ITU-T Rec. H.235.0 (such as H.235.1, H.235.2, H.235.3).

However, with the need to support an increasing number of parallel channels, the direct-routed call model with a gatekeeper could yield better performance and scalability properties. The advantage of this mode is the utilization of a gatekeeper for registration, admission, address resolution, and bandwidth control, while performing the call establishment directly between the end points in an end-to-end fashion.

This Recommendation describes the enhancements for the H.235.1 baseline and for H.235.3 hybrid security profiles to support direct-routed calls with gatekeeper(s).

7 Overview

The H.235.1 baseline, as well as the H.235.3 hybrid security profiles, apply a shared secret (after the first handshake) to assure message authentication and/or integrity in a hop-by-hop fashion using the gatekeeper as a trusted intermediate host. Using the direct-routed call model, a shared secret between two endpoints cannot be assumed. It is also not practical to use a pre-established shared secret to secure the communication since, in this case, all endpoints would have to know in advance which other endpoint will be called.

ITU-T Rec. H.235.4 addresses the scenario shown in Figure 1, where endpoints are attached to a gatekeeper and deploy direct-routed call signalling. The scenario assumes an unsecured IP network in the gatekeeper zone.

It is assumed that each endpoint has a communication relation and a security association with its gatekeeper, and that each endpoint has registered securely with the gatekeeper using either the baseline or the hybrid security profile.

Hence, the gatekeeper of the initiating endpoint (DRC1) or the gatekeeper of the terminating endpoint (DRC2) is able to provide a shared secret for the directly communicating endpoints using a Kerberos-like approach (see RFC 4120).

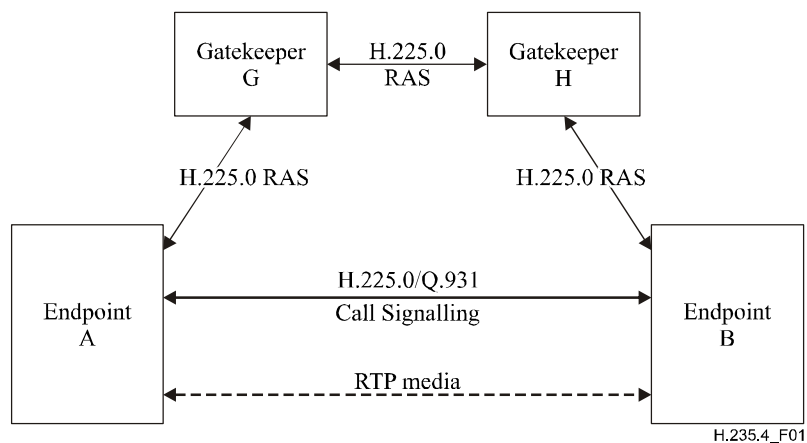


Figure 1/H.235.4 – Direct-routed call scenario

This Recommendation features two procedures, DRC1 and DRC2, for different environments.

Procedure DRC1 (see clause 9) is applicable in corporate environments where the gatekeepers are situated within different (local) sites but where the sites adhere to a common corporate security policy. In such an environment it is assumed acceptable that the originating gatekeeper G determines the effective security policy for a call to be established; thus the originating