# SLOVENSKI STANDARD
# SIST-TS TS 101 888-2 V4.1.1:2004

**01-april-2004**

---

**Harmonizacija telekomunikacij in internetnega protokola prek omrežij (TIPHON), 4. izdaja - Specifikacija varnostnega preskusa - 2. del: Okolje H.323**

Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Security Test Specifications; Part 2: H.323 Environment



**Ta slovenski standard je istoveten z: TS 101 888-2 Version 4.1.1**



---

**ICS:**

| | | |
|---|---|---|
| 33.020 | Telekomunikacije na splošno | Telecommunications in general |

**SIST-TS TS 101 888-2 V4.1.1:2004** **en**

# ETSI TS 101 888-2 V4.1.1 (2002-05)

*Technical Specification*

## Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Security Test Specifications; Part 2: H.323 Environment

Reference
DTS/TIPHON-06014-2R4

Keywords
H.323, IP, protocol, testing, security, VoIP

***ETSI***

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88



***Important notice***

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, send your comment to:
editor@etsi.fr

***Copyright Notification***

# Contents

Intellectual Property Rights ....4
Foreword ....4
1 Scope ....5
2 References ....5
3 Definitions and abbreviations ....5
3.1 Definitions ....5
3.2 Abbreviations ....5
4 Security Test Strategy ....6
5 H.235 annex D ....7
5.1 Overview ....7
5.2 Received message ....10
5.3 Separate Steps ....11
5.4 Test configurations ....12
5.4.1 Gatekeeper and Terminal ....12
5.4.2 Gatekeeper and Gateway ....12
5.4.3 Gatekeeper and Gatekeeper ....12
6 H.235 annex F ....13
7 Global Service Providers ....13
**Annex A (informative): Bibliography ....14**
History ....15

# Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

# Foreword

This Technical Specification (TS) has been produced by ETSI Project Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON).

The present document is part 2 of a multi-part deliverable covering Security Test Specifications, as identified below:

Part 1: "Framework";

**Part 2: "H.323 Environment".**

# 1 Scope

The present document is one part of the security testing standards for which a framework is available in TR 101 888-1.

The scope of the present document is to define the security test specifications for TIPHON Release 4 for the H.323 environment.

The security methods considered in the present document are related only to IP based networks. The signalling path and the media path in the SCN is considered to be secure ("Trust by wire").

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] ITU-T Recommendation H.225.0: "Call signalling protocols and media stream packetization for packet-based multimedia communication systems".

[2] ITU-T Recommendation H.235: "Security and encryption for H.Series (H.323 and other H.245-based) multimedia terminals".

[3] ITU-T Recommendation H.245: "Control protocol for multimedia communication".

[4] ITU-T Recommendation H.323: "Packet-based multimedia communications systems".



# 3 Definitions and abbreviations

## 3.1 Definitions

For the purpose of the present document, the terms and definitions given in the IUT-T Recommendations H.225.0 [1], H.235 [2], H.245 [3] and H.323 [4] apply.

## 3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

| | |
|---|---|
| A | Audio |
| D | Data |
| IP | Internet Protocol |
| SCN | Switched Circuit Networks |

# 4 Security Test Strategy

Security testing should be performed after a vendor has completed product and system testing with the ETSI testing standards.

The basic idea for security testing is to show the generation and insertion of the security bits into the specific parameters of the H.323 messages. Because this mechanism is exactly the same on the senders and the receiver's side, no distinction is necessary.

To test entities for their implementation of security two entities (that are already interworking) need to be connected. In the case of an incorrect security information it is necessary to go into the detail of the generation of the security bits. In order to be able to determine the reason for this failure the security tests strategy is just to look at the different steps of the generation and insertion of the security bits into the protocol elements. This is the only way to determine the failure.

The Security testing shall be performed for the following configurations:

- Signalling path:
  - Gatekeeper and Terminal;
  - Gatekeeper and Gateway;
  - Gatekeeper and Gatekeeper.
- Media path:
  - Terminal and Terminal;
  - Terminal and Gateway;
  - Gateway and Gateway.
- Global Service Providers:
  - BES and TRC;
  - BES and CH;
  - BES and CA.



The security testing shall be performed in three different parts where the first part deals with the security testing for the signalling path (Terminal, Gatekeeper, Gateway) using ITU-T Recommendation H.235 [2] annex D. The second part deals with the security aspects for the signalling path equivalent to the first but using ITU-T Recommendation H.235 [2] annex F and the media path using H.235. The third part handles the security testing from the BES to the global service providers.

# 5 H.235 annex D

## 5.1 Overview

Figure 1 shows the basic steps to be taken at the originating entity.

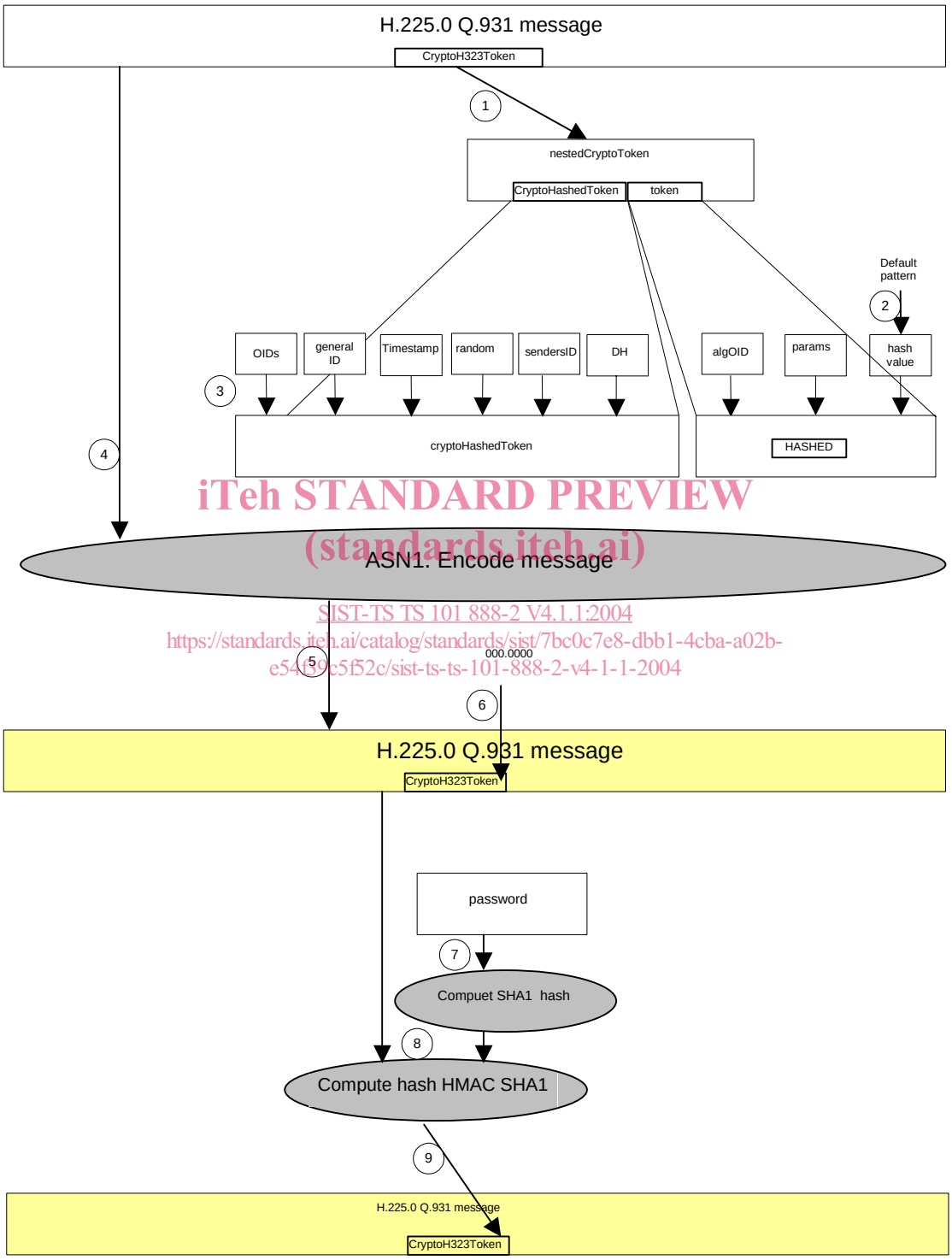




**Figure 1: Stepwise approach for sender**