

H.323 Annex J

Security for H.323 Annex F

1 Introduction

This annex describes security for H.323 Annex F simple endpoint types. The specified security profile is based upon recommendation H.235v2 and uses the featured baseline security profile of H.235 Annex D. The shown security profile in H.323 Annex J adopts recommendation H.235 for the purpose of simple endpoint types and their specific security requirements. The security profile selects appropriate security features from H.235 with its rich set of options.

The described text provides an overview on the security profile; H.235v2 Annex D provides all the technical and implementations details.

Basically, a **security simple endpoint type (security SET)** is a SET as defined by H.323 Annex F that implements additionally certain security features of this annex.

Currently, this annex focuses only on a “secure audio SET (SASET)” and leaves any other security simple endpoint types (e.g.; secure FAX SET, secure text terminal, secure Video SET etc) for further study.

This annex closes the open issue of security for SETs that was left for further study in chapter 8 of H.323 Annex F.

2 Specification Conventions

Some explanation is useful for understanding the terms used in this annex:

The annex applies the **baseline security profile** for a SASET (**secure audio simple endpoint terminal**). The baseline security profile provides basic security by simple means using secure password-based cryptographic techniques; the functionality provided should be implemented by each SASET. The baseline security profile may use the **voice encryption security profile** for achieving voice confidentiality if necessary. It is for further study, whether there will be other, more sophisticated security profiles for SASETs.

In order to avoid references to a trademark (RC2[®]), this document actually references an “RC2-compatible” encryption algorithm.

This document uses well-known security terms as key, key management and SET, which have different meanings in other contexts (e.g.; touch key pad, Q.931/Q932 feature key management, and Secure Electronic Transaction protocol).

3 Scope

This annex describes security for simple endpoint types. As shown in section 3 of H.323 Annex F, this currently includes:

- **Secure simple telephone terminal** (Secure Audio Simple Endpoint Type) — Defined in this annex (see chapter 6).

Any other security SETs are for further study.

4 Abbreviations

DES	Data Encryption Standard
GK	Gatekeeper
HMAC	Hashed Message Authentication Code
ITU	International Telecommunication Union
MAC	Message Authentication Code
RAS	Registration, Admission & Status
RTP	Real Time Protocol
SASET	Secure Audio Simple Endpoint Type
SET	Simple Endpoint Type
SHA	Secure Hash Algorithm

5 Normative References

H.225	ITU-T Recommendation H.225.0 Version 4, Call Signaling Protocols and Media Stream Packetization for Packet Based Multimedia Communications Systems, 2000.
H.235	(Draft) ITU-T Recommendation H.235 Version 2, Security and Encryption for H Series (H.323 and other H.245 based) multimedia terminals, 2000
H.245	ITU-T Recommendation H.245 Version 6, Control Protocol for Multimedia Communication, 2000.
H.323	ITU-T Recommendation H.323 Version 4, Packet Based Multimedia Communication Systems, 2000.
H.323 Annex F	ITU-T Recommendation H.323 Annex F “Simple Endpoint Types”, 1999.
RFC 2268	R. Rivest, “A Description of the RC2® Encryption Algorithm,” RFC-2268, March 1998.

6 Secure Audio Simple Endpoint Type (SASET)

This chapter describes a baseline for **secure audio simple endpoint types (SASETs)**. An example of a SASET is a secure simple phone.

6.1 Assumptions

The baseline security profile mandates the GK-routed model for secure H.323 Annex F SETs. SASETs and other H.323 entities that implement this security profile (e.g. GKs) are assumed to implement the fast connect procedure.

In accordance to Annex F the baseline security profile mandates the fast connect procedure with integrated key management elements but does not support H.245 tunneling. Thus, the baseline profile does not provide means for key update and synchronization using (tunneled) H.245 messages. SASETs implementing only the baseline security profile but still need some key-update mechanism should hang-up the call and re-connect and thereby obtain a new session key.

6.2 Overview

The baseline security is applicable in administered environments with symmetric keys/passwords assigned among the entities (SASETs-gatekeeper, gatekeeper-gatekeeper).

Table 1 summarizes all the procedures defined in H.235v2 Annex D.

Security Services	Call Functions							
	RAS		H.225.0		H.245 ¹	RTP		
Authentication	Password HMAC-SHA1-96		Password HMAC-SHA1-96		Password HMAC-SHA1-96			
Non-Repudiation								
Integrity	Password HMAC-SHA1-96		Password HMAC-SHA1-96		Password HMAC-SHA1-96			
Confidentiality						56-bit DES	56-bit RC2- com- patible	168- bit Triple -DES
Access Control								
Key Management	Subscription- based password assignment		Subscription- based pass- word assign- ment	authenti- cated Diffie- Hellman key-ex- change	Integrated H.235 session key management (key distribution, key update using 56- bit DES/ 56-bit RC2-compatible/ 168-bit Triple- DES)			

Table 1: Summary of Secure Audio Simple Endpoint Types (see H.235v2 Annex D)

For authentication and integrity, the user shall use a password-based scheme (blue area in table 1). The password-based scheme is highly recommended for authentication due to its simplicity and

¹ Embedded H.245 inside H.225.0 fast connect

ease of implementation. Hashing the fields in the H.225.0 messages is the recommended approach for integrity of the messages (also using the password scheme). SASETs realize authentication in conjunction with integrity using the same common security mechanism.

SASETs when deploying the voice encryption security profile (green area in table 1) shall implement 56-bit DES as the default encryption algorithm; SASETs may implement 168-bit Triple-DES while SASETs implementing exportable encryption may implement 56-bit RC2-compatible.

For voice confidentiality, the suggested scheme is encryption using RC2-compatible, DES or Triple-DES based on the business model and exportability requirement. Some environments that are offering already a certain degree of confidentiality may not require voice encryption. In this case, Diffie-Hellman key agreement and other key management procedures are not necessary as well.

Access control means are not explicitly described; they can be implemented locally upon the received information conveyed within H.235 signaling fields (ClearToken, CryptoToken).

This recommendation does not describe procedures for subscription-based password/secret key assignment with management and administration. Such procedures may happen by means that are not part of this annex.

SASETs may use back-end services according to the procedure described in H.235v2 Appendix I.4.6.