International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.235.6

(09/2005)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Systems aspects

H.323 security: Voice encryption profile with native H.235/H.245 key management

ITU-T Recommendation H.235.6

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 Recommendation H.235.6

H.323 security: Voice encryption profile with native H.235/H.245 key management

Summary

This Recommendation holds the security procedures for the voice encryption profile (formerly in Annex D/H.235) including the accompanying native H.235/H.245 key management.

In earlier versions of the H.235 sub-series, this profile was contained in the main body of H.235 and of its Annex D. 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.235.6 was approved on 13 September 2005 by ITU-T Study Group 16 (2005-2008) under the ITU-T Recommendation A.8 procedure.

Keywords

Authentication, certificate, digital signature, encryption, integrity, key management, multimedia security, security profile, voice encryption.

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.

CONTENTS

ITU-T Recommendation H.235.6

H.323 security: Voice encryption profile with native H.235/H.245 key management

1 Scope

This Recommendation specifies a security profile for voice encryption that uses the native H.235/H.245 key management. Procedures for both voice encryption and for the related native H.245 key management are specified within this Recommendation.

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 version 1 (1998), *Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals*.

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

– ITU-T Recommendation H.235 version 3 (2003), *Security and encryption for H series (H.323 and other H.245-based) multimedia terminals* plus Corrigendum 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.235.2 (2005), *H.323 security: Signature security profile*.

– ITU-T Recommendation H.235.3 (2005), *H.323 security: Hybrid security profile*.

– ITU-T Recommendation H.245 (2005), *Control protocol for multimedia communication*.

– ITU-T Recommendation H.323 (2003), *Packet-based multimedia communications systems*.

– ITU-T Recommendation H.323 Annex F (1999), *Simple endpoint types*.

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

ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.

– ITU-T Recommendation X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model*.

– ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

– ITU-T Recommendation X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*.

– IETF RFC 2198 (1997), *RTP Payload for Redundant Audio Data*.

– IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

– IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*.

– IETF RFC 2833 (2000), *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*.

– IETF RFC 3546 (2003), *Transport Layer Security Protocol (TLS) Extensions*.

– US National Institute of Standards, "Advanced Encryption Algorithm (AES)", *Federal Information Processing Standard, (FIPS)* Publication 197, November 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

– ISO/IEC 9797-1:1999, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher*.

– ISO/IEC 9797-2:2002, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function*.

– ISO/IEC 10118-3:2004, *Information Technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions*.

– ISO/IEC 10116:2006, *Information technology – Security techniques – Modes of operation for an n-bit block cipher*.

2.2 Informative references

[DES FIPS-46-2] US National Institute of Standards, Data Encryption Standard, *Federal Information Processing Standard*, (FIPS) Publication 46-2, December 1993, http://www.itl.nist.gov/fipspubs/fip46-2.htm.

[DES FIPS-74] US National Institute of Standards, Guidelines for Implementing and Using the Data Encryption Standard, *Federal Information Processing Standard*, (FIPS) Publication 74, April 1981, http://www.itl.nist.gov/div897/pubs/fip74.htm.

[DES FIPS-81] US National Institute of Standards, DES Modes of Operation, *Federal Information Processing Standard*, (FIPS) Publication 81, December 1980, http://www.itl.nist.gov/fipspubs/fip81.htm.

[FIPS PUB 180-1] NIST, FIPS PUB 180-1: *Secure Hash Standard*, April 1995 http://csrc.nist.gov/fips/fip180-1.ps.

[LI] ETSI TR 101 772 V1.1.2, Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Service Independent requirements definition; Lawful interception – top level requirements.

[OIW] Stable Implementation – Agreements for Open Systems Interconnection Protocols: Part 12 – OS Security; Output from the December 1994 Open Systems Environment Implementors' Workshop (OIW); http://nemo.ncsl.nist.gov/oiw/agreements/stable/OSI/12s_9412.txt.

[RFC2268] IETF RFC 2268 (1998), *A Description of the RC2$^{(r)}$ Encryption Algorithm*.

[RFC2405] IETF RFC 2405 (1998), *The ESP DES-CBC Cipher Algorithm With Explicit IV*.

[RFC2412] IETF RFC 2412 (1998), *The OAKLEY Key Determination Protocol*.

[WEBOIDs] http://www.alvestrand.no/objectid/top.html.

[Daemon] DAEMON (J.), *Cipher and Hash function design*, Ph.D. Thesis, Katholieke Universiteit Leuven, March 1995.

[ESP] IETF RFC 2406 (1998), *IP Encapsulating Security Payload (ESP)*.

[IKE] IETF RFC 2409 (1998), *The Internet Key Exchange (IKE)*.

[ISAKMP] IETF RFC 2408 (1998), *Internet Security Association and Key Management Protocol (ISAKMP)*.

[J.170] ITU-T Recommendation J.170 (2005), *IPCablecom security specification*.

[RTP] IETF RFC 3550 (2003), *RTP: A transport Protocol for Real-Time Applications*.

[Schneier] SCHNEIER (B.), *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd Edition, John Wiley & Sons, Inc., 1995.

[SRTP] IETF RFC 3711 (2004), *The Secure Real-Time Transport Protocol*.

3 Terms and definitions

For the purposes of this Recommendation, the definitions given in clauses 3/H.323, 3/H.225.0 and 3/H.245 apply. Some of the terms used in this Recommendation are also defined in ITU T Recs X.800 | ISO 7498-2, X.803 | ISO/IEC 10745, X.810 | ISO/IEC 10181-1 and X.811 | ISO/IEC 10181-2.

The **session key** for encrypting media streams, on the other hand, is generated by the master just for a specific RTP session (on an OLC), at longest for one call. The generated session key is encrypted with a key that is derived from the agreed Diffie-Hellman **shared secret** that both endpoints have computed. In this case, the DH-shared secret acts as Master Key for protection of the session key(s).

4 Symbols and abbreviations

This Recommendation uses the following abbreviations:

3DES Triple DES

AES Advanced Encryption Algorithm

ASN.1 Abstract Syntax Notation One

CBC Cipher Block Chaining

CFB Cipher Feedback

DES Data Encryption Standard

DH Diffie-Hellman

DTMF Dual Tone Multiple Frequency

ECB Electronic Code Book

EOFB Enhanced Output Feedback Mode

EP Endpoint

FEC Forward Error Correction

GK Gatekeeper

HMAC Hashed Message Authentication Code

IPsec	Internet Protocol Security
ITU	International Telecommunication Union
IV	Initialization Vector
KS	Salting Key in EOFB mode
MAC	Message Authentication Code
MC	Multipoint Controller
MCU	Multipoint Control Unit
MPS	Multiple Payload Stream
OFB	Output Feedback Mode
OID	Object Identifier
OLC	Open Logical Channel
RAS	Registration, Admission and Status
RC	Rivest Cipher
ROC	Roll-over Counter
RSA	Rivest, Shamir and Adleman
RTP	Real-Time Protocol
RTCP	Real-Time Control Protocol
SDU	Service Data Unit
SEQ	Sequence number
SHA	Secure Hash Algorithm
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSAP	Transport Service Access Point
UDP	User Datagram Protocol
XOR	Exclusive OR

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.

When deploying media encryption in conjunction with payload padding, the text sometimes says "the value of the pad should be determined by the normal convention of the cipher algorithm"; see e.g., 7.6.1, 8.3 and Figure I.7. This means that some cipher algorithms (e.g., DES) provide further implementation advice as to how the sender may choose the value of the padding byte(s). Examples could be random fill-in values, static values or other generated patterns. Whatever method is deployed does not impact interoperability, yet the security quality may well be different. This is considered as an implementation matter and is not specified any further in this Recommendation.

6 System overview

6.1 Voice encryption security profile

The voice encryption security profile is not an independent profile as is the baseline security profile. It is rather an option of the aforementioned security profile and may be used in conjunction with it. This profile also relies on certain security services as part of the call signalling and connection setup procedures; e.g., the Diffie-Hellman key agreement and other key management functions.

H.323 entities may implement this Recommendation for achieving voice confidentiality. Four encryption algorithms are offered: the suggested schemes are encryption using AES, RC2-compatible, DES or triple-DES based on the business model and exportability requirement. In addition to the CBC-encryption mode, H.323 entities may implement the EOFB stream-cipher encryption mode. Some environments that are already offering 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.

For optional voice confidentiality, the suggested scheme is encryption using AES-128, RC2-compatible, DES or triple-DES based on the business model and exportability requirement. Some environments that are already offering 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.

This Recommendation further profiles the list of candidate voice encryption algorithms that ITU-T Rec. H.235 version 2 Annex D or ITU-T Rec. H.235 version 3 Annex D had offered.

NOTE 1 – This further encryption algorithm profile takes into account the known cryptanalysis and security findings on the strengths of encryption algorithms and the change in crypto export policies. In particular, the profiling of encryption algorithms of this Recommendation takes into account interoperability requirements with systems complying with H.235 version 2 or 3.

H.323 entities that implement this Recommendation with version 4 of H.235 or higher shall offer 128-bit AES as the preferred voice encryption algorithm in their offered security capabilities to achieve highest performance and best security. Those H.323 entities may additionally and optionally offer also 168-bit Triple-DES as a voice encryption algorithm to achieve higher interoperability with H.323 systems that have implemented the voice encryption features in Annex D/H.235 Versions 2 and 3. Since 56-bit DES and 56-bit RC2-compatible (exportable) encryption algorithms are no longer considered sufficiently secure anymore, H.323 entities should not offer those particular weak encryption algorithms unless there is specific need for, such as achieving interoperability with voice encryption systems in Annex D/H.235 Versions 2 and 3.

H.323 entities that implement this Recommendation with version 4 of ITU-T Rec. H.235 shall prefer to accept offered 128-bit AES if allowed by their security policy. Those H.323 entities should additionally accept 168-bit Triple-DES if AES was not offered or is otherwise not allowed by their security policy. Those H.323 should not accept 56-bit DES or 56-bit RC2-compatible for security reasons, unless their security policy explicitly allows such insecure encryption algorithms, or exportability needs require such algorithms, and other more secure alternatives like 128-bit AES or 168-bit Triple DES are not offered.

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

This Recommendation does not describe procedures for subscription-based password/secret key assignment with management and administration. Such procedures may take place by means that are beyond the scope of this Recommendation.

The communication entities involved are able to implicitly determine usage of either the baseline security or the signature security profile by evaluating the signalled security object identifiers in the messages (**tokenOID**, and **algorithmOID**; see also clause 11).

Table 1 summarizes the security features of the voice encryption profile. The voice encryption profile is specified in clauses 7, 8, and 9.

Table 1/H.235.6 – Voice encryption profile

Security services	Call functions			
	RAS	**H.225.0**	**H.245**	**RTP**
Authentication and integrity				
Non-repudiation				
Confidentiality				56-bit DES; 56-bit RC2-compatible; 168-bit triple-DES; 128-bit AES; CBC-mode or EOFB-mode
Access control				
Key management		Authenticated Diffie-Hellman key-exchange	Integrated H.235 session key management (Authenticated Diffie-Hellman key-exchange, key update)	

The general procedure establishes a shared secret (Diffie-Hellman exchange) between the two communicating parties at connection initiation. This shared secret is then used to protect (a set of) media keys that are used to encrypt the media (RTP) sessions.

The voice encryption security profile is an optional enhancement to the baseline security profile and to the signature security profile; its use can be negotiated as part of the terminal security capability negotiation. In environments where voice confidentiality is assured by other means, there is no need to implement the media encryption and the related key management procedures (Diffie-Hellman key agreement, key update and synchronization).

The encryption algorithms chosen are AES, RC2-compatible, DES and triple-DES.

NOTE 2 – Since an implementation of triple-DES can also be used for the DES algorithm, this results in a compact implementation.

Irrespective of the choice of the specific media encryption algorithm, the options below shall be followed explicitly.

- Initialization Vector (IV) generated, if needed, as specified in 9.3.1.
- Padding, if needed, is to occur as described in 9.3.2.

The audio payload shall be encrypted using the negotiated encryption algorithm ("X", "Y", "Z3" or "Z") according to the procedures described in clause 9 and in 9.3, and the ciphertext padding methods of clause I.1. The audio payload may be encrypted using the negotiated encryption algorithm ("X1", "Y1", "Z1" or "Z2") operating in a stream cipher mode (EOFB).

7 H.245 signalling and procedures

In general, the privacy aspects of media channels are controlled in the same manner as any other encoding parameter; each terminal indicates its capabilities, the source of the data selects a format to use, and the receiver acknowledges or denies the mode. All transport-independent aspects of the mechanism such as algorithm selection are indicated in generic logical channel elements. Transport specifics such as key/encryption algorithm synchronization are passed in transport-specific structures.

7.1 Secure H.245 channel operation

Assuming that the connection procedures indicate a secure mode of operation, the negotiated handshake and authentication shall occur for the H.245 control channel before any other H.245 messages are exchanged. If negotiated, any exchange of certificates shall occur using any mechanism appropriate for the H-series terminal(s). After completing the securing of the H.245 channel, the terminals use the H.245 protocol in the same manner that they would in an insecure mode.

7.2 Unsecured H.245 channel operation

Alternatively, the H.245 channel may operate in an unsecured manner and the two entities open a secure logical channel with which to perform authentication and/or shared-secret derivation. For example, TLS (RFC 2246, RFC 3546) or IPsec (RFC 2401) may be utilized by opening a logical channel with the **dataType** containing a value for **h235Control**. This channel could then be used to derive a shared secret which protects any media session keys or to transport the **EncryptionSync**.

7.3 Capability exchange

Following the procedures in 5.2/H.245 (Capability exchange procedures) and the appropriate H-series system Recommendation, endpoints exchange capabilities using H.245 messages. These capability sets may now contain definitions which indicate security and encryption parameters. For example, an endpoint might provide capabilities to send and receive H.261 video. It may also signal the ability to send and receive encrypted H.261 video.

Each encryption algorithm that is utilized in conjunction with a particular media codec implies a new capability definition. As with any other capability, endpoints may supply both independent and dependent encrypted codecs in their exchange. This will allow endpoints to scale their security capabilities based upon overheads and resources available.

After capability exchange has been completed, endpoints may open secure logical channels for media in the same manner that they would in an insecure manner.

7.4 Master role

The H.245 master-slave is used to establish the master entity for the purpose of bidirectional channel operation and other conflict resolution. This role of master is also utilized in the security methods. Although the security mode(s) of a media stream is set by the source (in deference to the capabilities of the receiver), the master is the endpoint which generates the encryption key. This generation of the encryption key is done, regardless of whether the master is the receiver or the source of the encrypted media. In order to allow for multicast channel operation with shared keys, the MC (also the master) should generate the keys.

7.5 Logical channel signalling

Endpoints open secure media logical channels in the same manner that they open unsecured media logical channels. Each channel may operate in a completely independent manner from other channels – in particular where this pertains to security. The particular mode shall be defined in the **OpenLogicalChannel dataType** field. The initial encryption key shall be passed in either the **OpenLogicalChannel** or **OpenLogicalChannelAck** depending on the master/slave relationship of the originator of the **OpenLogicalChannel**.

The **OpenLogicalChannelAck** shall act as confirmation of the encryption mode. If the **openLogicalChannel** is unacceptable to the recipient, either **dataTypeNotSupported** or **dataTypeNotAvailable** (transient condition) shall be returned in the cause field of the **OpenLogicalChannelReject**.

During the protocol exchange that establishes the logical channel, the encryption key shall be passed from the master to the slave (regardless of who initiated the **OpenLogicalChannel**). For media channels opened by an endpoint (other than the master), the master shall return the initial encryption key and the initial synchronization point in the **OpenLogicalChannelAck** (in the **encryptionSync** field). For media channels opened by the master, the **OpenLogicalChannel** shall include the initial encryption key and the synchronization point in the **encryptionSync** field.

7.6 Fast connect security

Endpoints may deploy the fast connect procedure (see clauses 8.1.7 and 8.1.7.1/H.323) using the fast start element for securely exchanging key material (master key and session encryption keys). The procedures given in 7.6.1 describe "plain" fast start that does not use multiple offered encryption algorithms whereas 7.6.1.1 describes the particular case of fast start with multiple offered encryption algorithms that enables more compact message encoding.

7.6.1 Unidirectional fast start security

This procedure describes how to establish a (half-duplex) unidirectional security logical channel from the caller to the callee.

Procedures of the caller

The caller (source of the SETUP) presents both its DH token, and the supported FastStart structures. The DH token shall be conveyed within an embedded ClearToken as part of a CryptoToken, or as a separate ClearToken, see also 7.8. During the SETUP-to-CONNECT sequence, a Diffie-Hellman (DH) exchange shall be performed: this seeds both endpoints with a shared secret. The **ClearToken** field of the **CryptoToken** fields shall contain a **dhkey**, used to pass the parameters as specified in this Recommendation. **halfkey** contains the random public key of one party, **modsize** contains the DH-prime and **generator** contains the DH-group. The DH parameters to be used are indicated in Table 4. For more details, please refer to [RFC2412], Appendix E2.

NOTE 1 – Since the H.225.0 messages are authenticated (as described earlier by procedure I), the DH exchange is an authenticated one.

In either direction with a H.225.0 call signalling message carrying a Diffie-Hellman half-key, when identification information is available, the caller or callee, when being registered, shall also include a separate end-to-end **ClearToken** with **sendersID** set to the endpoint identifier of the sender and **tokenOID** set to "E". Any intermediate H.323 signalling entity shall forward that particular end-to-end token unmodified.

The FastStart structures hold the offered open logical channels with the proposed security capabilities. Both H235Cap and nonH235Cap channels should be offered. During the H.245 Cap exchange, endpoints present **H235SecurityCapability** entries for the codecs that they support. Each codec is associated with a separate H.235 security capability. According to Table 6, these capabilities should indicate support for 128-bit AES-CBC (OID – "Z3"), 56-bit RC2-compatible-

CBC (OID – "X"), should indicate support for 56-bit DES-CBC (OID – "Y") and may indicate support for 168-bit triple-DES-CBC (OID – "Z"), or 168-bit Triple-DES-EOFB (OID – "Z1"), RC2-compatible-EOFB (OID – "X1"), DES-EOFB (OID – "Y1") or AES-EOFB (OID – "Z2").

OpenLogicalChannel conveys both **forwardLogicalChannelParameters** and **reverseLogicalChannelParameters** with **dataType** providing **h235Media** with **encryptionAuthenticationAndIntegrity** where in the **encryptionCapability** at most one **MediaEncryptionAlgorithm** shall be present.

For the security relationship's purpose, the callee is the *a priori* master, see also 7.4.

The caller should set **mediaWaitForConnect** to true, to ascertain that session key material is available and received encrypted media can be decrypted. In scenarios, where "early media" is desired, such that the callee transmits encrypted or non-encrypted media simultaneously with sending the response message and encryption key material, the caller should be prepared not to be able to decrypt the contents unless key material is available.

NOTE 2 – In this case, if the callee sends encrypted media to the caller (which theoretically it may do, because it has the caller's RTP/RTCP addresses), the caller will not be able to decipher it without the shared secret provided in the (Alerting, Call Proceeding) Connect message.

Procedures of the callee

During FastStart, the callee presents its DH token (see also 7.8) and the accepted FastStart structures. In case the Diffie-Hellman procedure is applied, it is recommended that the callee returns its DH token as part of the response message at the earliest opportunity; i.e., in the response message immediately following the SETUP. This allows the caller to compute the master key from the DH shared secret and to be prepared for receiving the session key and encrypted media.

NOTE 3 – In case there is no encryption algorithm available at both sides, the media stream may be left unencrypted or the connection may be aborted, depending on the security policy.

Each entity shall take appropriate least significant bits from the common shared Diffie-Hellman secret for the key encryption key (master key); i.e., the 56 least significant bits of the Diffie-Hellman secret for OID "X", OID "X1", OID "Y1" or OID "Y" and the 168 least significant bits of the Diffie-Hellman secret for OID "Z", OID "Z1" or OID "Z2" and the 128 least significant bits of the Diffie-Hellman secret for OID "Z3" or OID "Z2", see also Table 6.

OpenLogicalChannel(Ack) responses are issued with the (master) created session key included in the **encryptionSync** field. This **encryptionSync** holds the session key for the directed logical channel from caller to callee. Key transport shall proceed according to the procedure described in 8.3, using either **KeySyncMaterial** or **V3KeySyncMaterial** (see 8.3.1). The session key shall be encrypted with the DH shared secret in a manner described below.

NOTE 4 – There is no prescribed method for generating the session keys, which are utilized to encrypt the media. The generation of these values is an implementation matter affected by local resources, policy, and the encryption algorithm to be used. Care should be taken to avoid generation of weak keys.

Using the procedure of 8.3, the encrypted session key shall be carried in the **H.235Key**/**sharedSecret** within the **encryptionSync** field. The session key shall be carried in the **keyMaterial** field of the **KeySyncMaterial**, if not a multiple of the block size, shall be padded to a multiple of blocks before encryption. The value of the pad should be determined by the normal convention of the cipher algorithm. The (padded) **KeySyncMaterial** shall be encrypted using:

– 56 bits of the shared secret, starting with the least significant bits from the Diffie-Hellman secret for OID "X", OID "X1" , OID "Y1" or OID "Y";

– all the bits of the shared secret for OID "Z2", OID "Z" or OID "Z1" starting with the least significant bits from the DH secret.

Alternatively and preferably, the improved key transport according to 8.3.1 should be used when possible due to the outcome of the version 3 indicating procedure (see 8.2).

In case a full duplex secured media channel out of two unidirectional channels is to be established using fast start, the callee shall open a second logical channel towards the caller. This logical channel shall be signalled in a separate fastStart element. Using the available DH shared secret as master key, the callee includes a different session key for that logical channel within **encryptionSync**.

7.6.1.1 Using multiple encryption algorithms in fast connect

The negotiation of media encryption as part of fast connect procedures leads to an inefficient expansion of the number of **OpenLogicalChannel** elements in the **fastConnect** element of a SETUP message. This occurs because a separate **OLC** is required for each combination of codec (**dataType**) and encryption algorithm (including "none").

The encryption algorithm to be applied to a media stream is specified through inclusion of the **dataType.h235Media.encryptionAuthenticationAndIntegrity.encryptionCapability dataType** in the **OLC**. H.235v2 practice is to include only a single **MediaEncryptionAlgorithm** in the **encryptionCapability**, although the latter element is defined as a sequence of the former elements. This procedure permits the inclusion of a preference-ordered sequence of encryption capabilities in each offered **OLC**. The receiver of the **OLC** shall then select a single algorithm from among those offered, and shall return the **OLC** with only the selected algorithm present (along with the appropriate transport addresses and encryption key information.)

In order to provide the maximum efficiency, the Object ID "NULL-ENCR" (see Table 2) represents the "null" encryption algorithm which means that no encryption operation is to take place. Using this particular method requires only one **OLC** per offered codec per direction.

Table 2/H.235.6 – Object identifier for NULL encryption

Object identifier reference	Object identifier value	Description
"NULL-ENCR"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 26}	Indicates the "NULL encryption algorithm"

Procedure for the caller (see 8.1.7.1/H.323)

If an offered **dataType** element specifies encryption via the **h235Media** choice, the included **encryptionAuthenticationAndIntegrity** element may include an **encryptionCapability** element containing multiple encryption algorithms (including the NULL algorithm). This construct shall be taken to offer a choice of any one of the specified algorithms for encryption of the associated media capability.

Procedure for the callee (see 8.1.7.1/H.323)

If multiple encryption algorithms are offered for a channel, the called endpoint must select one and modify the **OpenLogicalChannel** to remove the others.

7.6.2 Bidirectional fast start security

Security for bidirectional T.120 data channels is for further study.

7.7 Encrypted H.245 DTMF

Endpoints may choose to send encrypted DTMF (RFC 2833) signals to achieve confidentiality. Using the session encryption key, endpoints may encrypt the DTMF (RFC 2833) signals in **UserInputIndication** as:

- Encrypted basic string: **encryptedAlphanumeric**;
- Encrypted iA5 string: **encryptedSignalType** within **signal**;
- Encrypted general string: **encryptedAlphanumeric** within **extendedAlphanumeric**.

NOTE 1 – The additional parameters for RTP in the iA5 string with timestamps and logical channel numbers or the signal update with the tone duration are not encrypted, as they are considered not to convey sensitive information.

The negotiated capability **secureDTMF** relates to an encrypted iA5 string.

The key management as specified by clause 6.1 should be applied to yield a session encryption key. That session encryption key shall be used to encrypt the H.245 DTMF (RFC 2833) signals.

NOTE 2 – This does not necessarily imply that the session key should be applied for RTP payload encryption as well.

However, when also using the DTMF (RFC 2833) via RTP by setting the **rtpPayloadIndication** flag, it is highly recommended that the RTP payload be secured using the voice encryption profile of 6.1.

Table 3 provides the available encryption algorithms (DES, 3DES or AES) which should deploy EOFB (incl. OFB as a special case, see 8.4). To avoid potential padding of the DTMF (RFC 2833) characters, CBC, CFB or other block chaining modes that may make padding necessary, are not recommended for encryption of DTMF (RFC 2833) signals.

7.7.1 Encrypted basic string

If **encryptedBasicString** in **UserInputCapability** has been selected, then **encryptedAlphanumeric** shall indicate the applied encryption algorithm within **algorithmOID**, **paramS** holds the initial value for the encryption operation. The encrypted alphanumeric string shall be placed in **encrypted**.

7.7.2 Encrypted iA5 string

If **encryptedIA5String** in **UserInputCapability** has been selected, then **encryptedSignalType** shall hold the encrypted **ClearSignalType** where **sig** carries the plaintext **signalType** character. **signalType** shall hold a dummy "!" which shall be discarded by the recipient.

algorithmOID shall indicate the applied encryption algorithm, **paramS** holds the initial value for the encryption operation.

7.7.3 Encrypted general string

If **encryptedGeneralString** in **UserInputCapability** has been selected, then **encryptedAlphanumeric** within **extendedAlphanumeric** shall indicate the applied encryption algorithm within **algorithmOID**, while **alphanumeric** shall hold an empty string and **paramS** holds the initial value for the encryption operation.

7.7.4 List of object identifiers

Table 3/H.235.6 – Object identifiers for H.245 DTMF encryption

Object identifier reference	Object identifier value	Description
"DES-EOFB-DTMF"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 12}	H.245 DTMF encryption with DES-56 in EOFB mode
"3DES-EOFB-DTMF"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 13}	H.245 DTMF encryption with 3DES-168 in EOFB mode
"AES-EOFB-DTMF"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 14}	H.245 DTMF encryption with AES-128 in EOFB mode

7.8 Diffie-Hellman operation

This Recommendation supports the Diffie-Hellman protocol for end-to-end key agreement. Depending on the situation, the negotiated Diffie-Hellman key may act as master key (see 6.1) or as a dynamic session key (ITU-T Recs H.235.3 and H.530).

The Diffie-Hellman system is characterized by the system parameters g and p where p shall be a large prime and g denotes the generator of the multiplicative group modulo p or of a strong subgroup modulo p. g^x mod p denotes the (public) Diffie-Hellman half-key of the caller while g^y mod p denotes the (public) Diffie-Hellman half-key of the callee. RFC 2412 provides further background information and advice how to choose secure Diffie-Hellman parameters.

ITU-T Rec. H.235.0 conveys a Diffie-Hellman instance (g, p, g^x) encoded within a **ClearToken** where **dhkey** holds the **halfkey** g^x mod p (resp. g^y mod p) for some secret random x (resp. y), the prime p in **modsize** and the **generator** g. A special case is the triplet (0, 0, 0) or an empty **dhkey** that does not represent any DH-instance but shall be used in signalling that the voice encryption profile is not being used.

Often, the DH-system parameters p and g are fixed for a set of applications with well-defined values, yet end systems may also choose their own set of parameters. The callee should be aware of the fact that non-standard DH-parameters may provide less security than the parameters look alike at first sight; e.g., the caller might have chosen a non-prime, or g generates just a smaller subgroup. While extensive parameter testing is unfeasible in practice, it is up to the security policy of the callee whether to accept or reject such offers.

For the fixed DH system parameters, a shorthand characterization through an object identifier may yield more compact encoded messages than including literal values. A **ClearToken** that carries a DH-instance with fixed, standardized DH parameters, may reference the DH instance with a DH-OID in the **tokenOID** field; unless the **tokenOID** is used for other purposes (such as in clause 7/H.235.1 for a distinguished **CryptoToken**). The sender may additionally include the literal DH values but need not do so.

In case several DH-instances are to be indicated each through a DH-OID, the DH-parameters in a distinguished **CryptoToken** (which is being occupied by H.235.1) shall be omitted by leaving **dhkey** absent, and all DH-instances shall then be carried within separate **ClearTokens** where the **tokenOID** holds the DH-OID, and **dhkey** may be left absent; any other fields within that **ClearToken** shall not be used.

NOTE 1 – This does not rule out the possibility to convey a DH instance in a distinguished **CryptoToken** or other available **ClearTokens** by literally including the DH parameter values.

In case a non-standard DH-instance is to be indicated, the DH-OID "DHdummy" shall be used and the non-standard DH-group parameters shall be explicitly provided in the **ClearToken**.

The caller may submit one or several **ClearTokens** each conveying a different Diffie-Hellman instance. The caller is encouraged to provide as many DH instances as possible as his/her security policy permits. This allows the callee to choose an appropriate instance for the response, thereby increasing the likelihood of finding a successful common parameter set.

The callee shall select and accept a single DH instance (if at all) that it chooses from the unordered set of DH instances provided by the caller in the SETUP message. In case the callee is able to select a DH instance that matches his/her own security needs, the callee shall not modify a proposed DH instance or return one that was not sent by the caller. The strength of the encryption algorithms available to both EPs during the call should correspond to the strength provided by the chosen DH instance that is returned by the callee; see Table 4. The callee shall indicate the chosen DH instance in the response message.

In case the callee rejects any of the proposals for security reasons or due to lack of processing capabilities, the callee shall leave **dhkey** absent in the response message.

The callee shall include its DH token in the SETUP-to-CONNECT response. The callee may include its DH token in the immediate response message following SETUP, or may include the DH token at some later stage, but at latest in the CONNECT message.

NOTE 2 – There are several aspects to be taken into account as to when the callee may include the DH token(s) during the SETUP-to-CONNECT responses: the response time, the processing load upon the callee, capability of early media and other aspects. These issues are considered implementation dependent.

For some reasons, however, certain routing GKs may not deliver all SETUP-to-CONNECT responses to the caller. Thus, one or more H.225.0 call signalling response messages, including a possible DH token, may be dropped and would not arrive at the caller. The caller would then be unable to compute the DH master key and media session key(s). To prevent such cases, the callee should always include the same DH token in each SETUP-to-CONNECT response message.

In cases where the DH-OID indicates a different DH-instance than is actually being conveyed within **modsize** and **generator**, the literal values conveyed within **modsize** and **generator** shall take precedence over the DH-OID in the token. For the response, the callee should replace the conflicting DH-OID with the static DH-OID, e.g., "DH1024," that corresponds to the **modsize** and generator or "DHdummy" if there is no corresponding DH-OID.

7.8.1 Requesting renegotiation of DH parameters in the middle of the call

H.323 gatekeeper may request renegotiation of the DH parameters in the middle of the call using the procedures defined in this clause. Such renegotiation procedure may be needed to establish DH key agreement between an endpoint already connected to the gatekeeper and an endpoint to be connected (see Figure 1). The procedure for renegotiating the Diffie-Hellman parameters is needed in supporting several supplementary services. All the procedures defined in this clause shall be performed only when the H.323 endpoint are in "transmitter side paused" state, defined in 8.4.6/H.323.

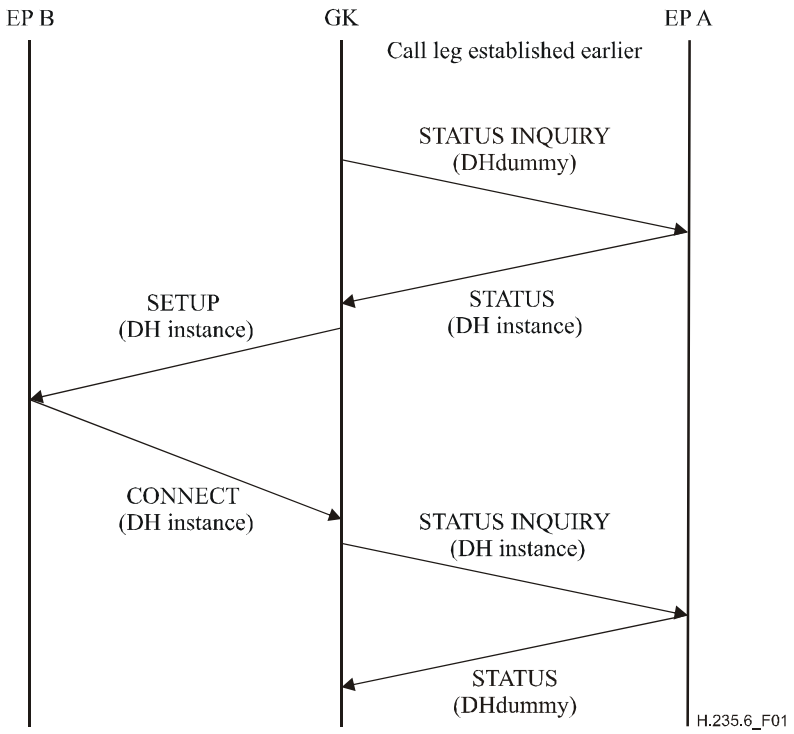


Figure 1/H.235.6 – Usage of "Requesting DH parameters in the middle of the call" for supplementary services

To request DH parameters in the middle of the call H.323 entity shall send STATUS INQUIRY message containing **ClearToken** field with DH-OID "DHdummy" in the **tokenOID** field and the rest of the fields omitted.

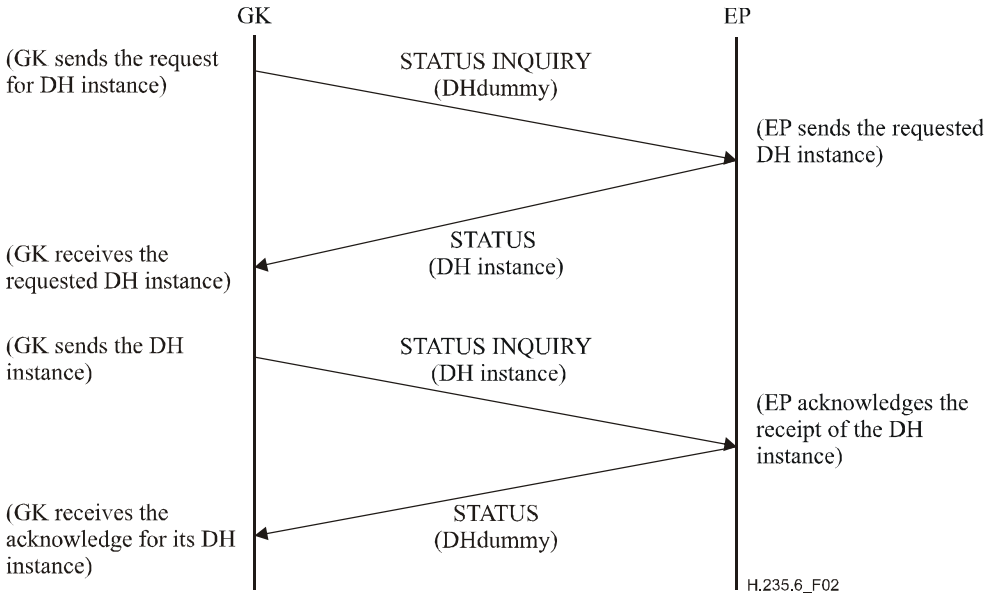


Figure 2/H.235.6 – Requesting DH parameters in the middle of the call

If an H.323 entity receives the STATUS INQUIRY message containing **ClearToken** field with DH-OID "DHdummy" in the **tokenOID** field, the H.323 endpoint shall respond with STATUS message containing the set of DH instances, see Figure 2. The DH instances shall be specified in this STATUS message according to the rules defined in 7.8 for the SETUP message.

NOTE 1 – The H.323 entity which does not support this procedure is supposed to respond to STATUS INQUIRY with STATUS message without DH instances.

To convey the accepted DH instance in the middle of the call, the H.323 entity shall send STATUS INQUIRY containing the accepted DH instance, see Figure 2. The DH instances shall be specified in this STATUS INQUIRY message according to the rules defined above in 7.8 for the response to the SETUP message.

If an H.323 endpoint receives such a STATUS INQUIRY message containing **ClearToken** field with a DH instance, the H.323 endpoint shall respond with STATUS message containing **ClearToken** field with DH-OID "DHdummy" in the **tokenOID** field and the rest of the fields omitted.

NOTE 2 – The H.323 entity which does not support this procedure is supposed to respond to STATUS INQUIRY with STATUS message without DH instances.

The H.323 endpoint receiving the STATUS INQUIRY message with DH instance shall recalculate the DH shared secret from this DH instance and the latest set of DH instance(s) which has been sent by this H.323 endpoint in the particular call.

If an H.323 GK receives a STATUS INQUIRY message containing **ClearToken** field with a DH instance, or with DH-OID "DHdummy" in the **tokenOID** field, then, with the exception of the several cases outlined below, it shall forward the message to the second leg of the call in context of which the message has been received.

If an H.323 GK receives a STATUS response to the STATUS INQUIRY message it has forwarded, the GK shall forward back the STATUS message to the call leg on which the STATUS INQUIRY message has been received.

If an H.323 GK waiting for response to the STATUS INQUIRY message containing **ClearToken** field, with DH-OID "DHdummy" in the **tokenOID** field which it has sent receives STATUS INQUIRY message containing **ClearToken** field with DH-OID "DHdummy" in the **tokenOID** field and with CRV flag set to value 1, then the GK shall respond with the STATUS message containing **ClearToken** field with DH-OID "DHdummy" in the **tokenOID** field (see Figure 3).

If an H.323 GK receives a STATUS INQUIRY message containing **ClearToken** field with a DH instance or with DH-OID "DHdummy" in the **tokenOID** field while the second leg of the call is not established, the GK shall wait establishment of the second leg of the call, send empty capability set on this call leg and then forward to it the received STATUS INQUIRY message (see Figure 3).

An H.323 GK shall not initiate procedures defined in this clause after it has sent STATUS message containing a DH instance and before it has received the STATUS INQUIRY message containing a DH instance.

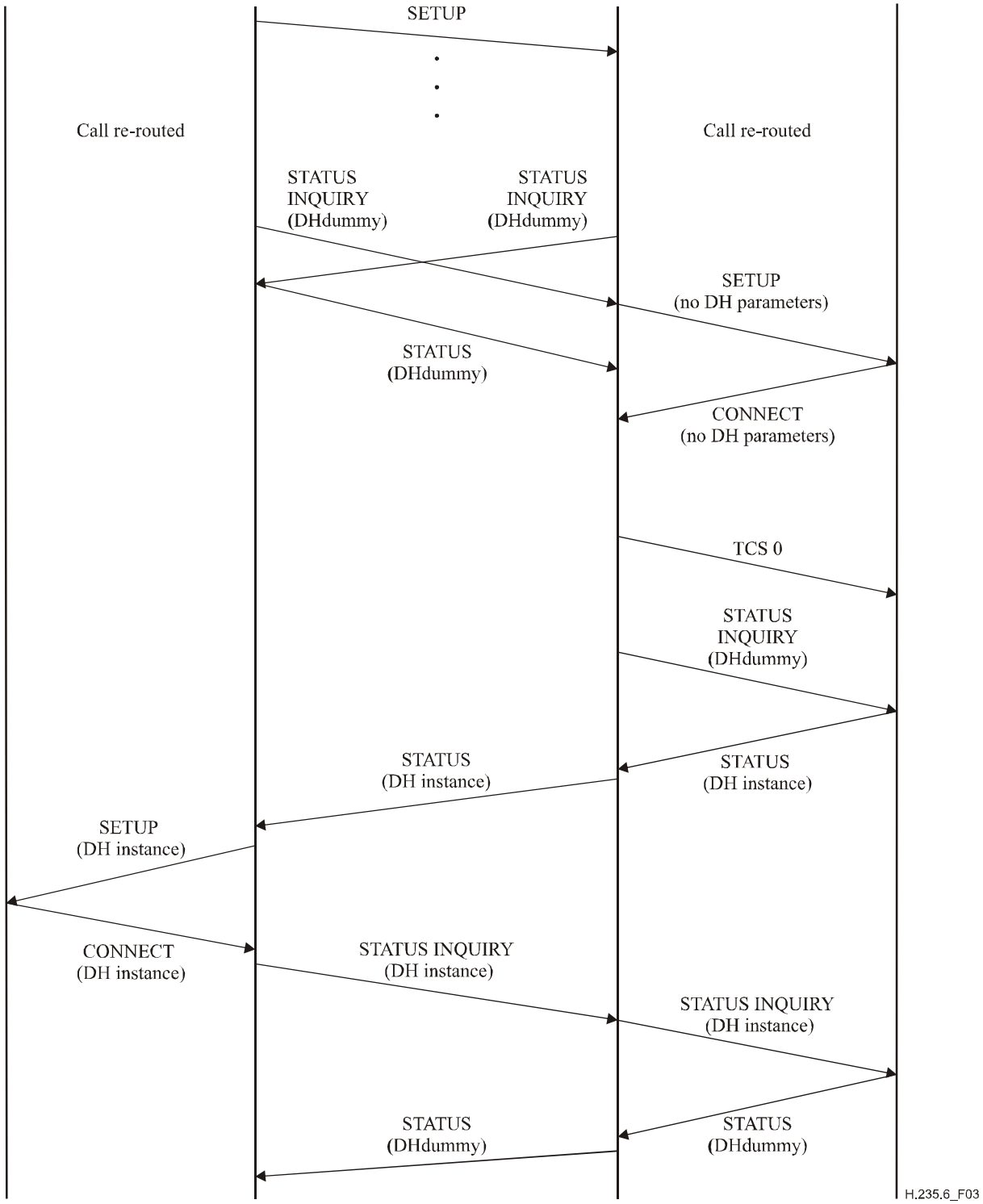


Figure 3/H.235.6 – Usage of "Requesting DH parameters in the middle of the call" for simultaneous call re-route by both GKs

8 Signalling and procedures

The procedures outlined in clause 8/H.323 (Call signalling procedures) shall be followed. The H.323 endpoints shall have the ability to encode and recognize the presence (or absence) of security requirements (for the H.245 channel) signalled in the H.225.0 messages.

In the case where the H.225.0 channel itself is to be secured, the same procedures in clause 8/H.323, shall be followed. The difference in operation is that the communications shall only occur after

connecting to the secure TSAP identifier and using the predetermined security modes (e.g., TLS (RFC 2246, RFC 3546)). Due to the fact that the H.225.0 messages are the first exchanged when establishing H.323 communications, there can be no security negotiations "in band" for H.225.0. In other words, both parties must know *a priori* that they are using a particular security mode. For H.323 on IP, an alternative Well Known Port (1300) is utilized for TLS (RFC 2246, RFC 3546) secured communications.

One purpose of H.225.0 exchanges as they relate to H.323 security is to provide a mechanism to set up the secure H.245 channel. Optionally, authentication may occur during the exchange of H.225.0 messages. This authentication may be certificate- or password-based, utilizing encryption and/or hashing (i.e., signing). The specifics of these modes of operation are described in clauses 8.1 to 8.2.3/H.235.0.

An H.323 endpoint that receives a SETUP message with the **h245SecurityCapability** set shall respond with the corresponding acceptable **h245SecurityMode** in the CONNECT message. In the cases in which there are no overlapping capabilities, the called terminal may refuse the connection by sending a **Release Complete** with the reason code set to ***SecurityDenied***. This error is intended to convey no information about any security mismatch and the calling terminal will have to determine the problem by some other means. In cases where the calling terminal receives a CONNECT message without sufficient, or an acceptable, security mode, it may terminate the call with a **Release Complete** with ***SecurityDenied***. In cases where the calling terminal receives a CONNECT message without any security capabilities, it may terminate the call with a **Release Complete** with ***undefinedReason***.

If the calling terminal receives an acceptable **h245Security** mode, it shall open and operate the H.245 channel in the indicated secure mode. Failure to set up the H.245 channel in the secure mode determined here should be considered a protocol error and the connection terminated.

8.1 Revision 1 compatibility

A security capable endpoint shall not return any security-related fields, indications or status to the non-security capable endpoint. If a caller receives a SETUP message that does not contain the **H245Security** capabilities and/or authentication token, it may return a **ReleaseComplete** to refuse the connection; but it shall use the reason code of ***UndefinedReason*** in this case. In a corresponding manner, if a caller receives a CONNECT message without an **H245SecurityMode** and/or authentication token having sent a SETUP message with **H245Security** and/or authentication token, it may also terminate the connection by issuing a **ReleaseComplete** with a reason code of ***UndefinedReason***.

8.2 Version 3 feature indication

H.235 version 3 and higher endpoints provide improved security procedures on the media path that H.235 version 1 and H.235 version 2 do not support. These improved security procedures are:

- the improved key transport (**V3KeySyncMaterial**, see 8.3.1);
- the improved key update, see 8.6.2.

Since endpoints usually do not know about their mutual support of H.235 version 3 or higher, an explicit version indication is added during call setup.

H.235 version 3 and higher endpoints should always use the procedure described in this clause for determining version 3 capability (improved key transport, improved encryption sync). Depending on the outcome of the logical signalling procedure, the end points may use the procedures (see 8.3) for backward compatibility with H.235 version 1 or with version 2 end points.

In order to indicate whether to use the improved H.235 version 3 procedures, the calling and the called endpoint shall include an additional **ClearToken** indicating version 3 capability during the

call signalling (SETUP, CONNECT, etc.). Absence of such a **ClearToken** would indicate support of only H.235 version 1 or version 2. In this case, the endpoint shall use the procedure of 8.3. Otherwise, the endpoint may use the improved procedures as described in 8.3.1, or use the H.235 version 1 or version 2 procedure of 8.3.

That **ClearToken** shall use **tokenOID** set to "V3" and is assigned the following value.

"V3"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 24}	Version 3 capability indicator in ClearToken during call signalling.

Any other fields in that **ClearToken** shall remain unused, unless being used to convey DH parameters.

8.3 Key transport

The master shall generate session key material and distribute it to the peer(s). Two procedures are offered for key transport:

- A procedure primarily for H.235 version 1 or version 2 endpoints; described in this clause.
- An improved procedure for H.235 version 3 and higher endpoints, described in 8.3.1.

H.235 version 1 or version 2 endpoints apply the following procedure for session key transport:

KeySyncMaterial holds the end point identifier of the master within **generalID** and carries the session key material within **keyMaterial**. The **generalID** value should be included to provide a minimal level of authentication of the source of the session key (see also 8.6). The recipient should verify correctness of the received **generalID**.

NOTE – This Recommendation assumes that each endpoint has registered with a gatekeeper and has obtained an endpoint identifier that can be conveyed within **generalID**. This Recommendation does not support scenarios without gatekeepers; this remains for further study.

KeySyncMaterial shall be encrypted using the negotiated master key. The **KeySyncMaterial** shall always be padded to a multiple of blocks before encryption where the last octet shall be set to the number of padding octets (including the last). The value of the pad should be determined by the normal convention of the cipher algorithm. The encryption result shall be stored in **sharedSecret** of **H235Key**.

8.3.1 Improved key transport in H.235 version 3

It has been observed that the ASN.1 syntax definition of **KeySyncMaterial** and the way that the ENCRYPTED{} operation is applied to the data in H.235 versions 1 and 2, reveals plenty of known plaintext: first of all, the **generalID** of the master, but also some known coding bits for the structure. The **generalID**, even while being encrypted, is known from other non-encrypted parts of the signalling message (e.g., **senderID**). It is believed that the presence of such known plaintext significantly weakens the security scheme in such a way that an attacker could more easily crack the session key by "brute force", especially for a block cipher that has a shorter block size, such as DES-56 or RC2-compatible.

Further, version 3 of H.235 shall be capable of transporting additional key material:

- Secure transport of a salting key to the peer(s). Such a salting key is being introduced for the enhanced OFB mode; see 8.4.

H.235 version 3 extends **H235Key** with **secureSharedSecret** containing **V3KeySyncMaterial** that holds the following parameters:

generalID holds the endpoint identifier of the originating sender if available, otherwise this field remains unused.

algorithmOID indicates the applied encryption algorithm and the operation mode.

paramsS holds the initialization value, that is applied for encryption of the conveyed key(s).

NOTE 1 – The IV within **paramS** should not be confused with the per RTP packet IV that is not being signalled. **ClearSalt** optionally holds an unencrypted salting key for session key encryption (e.g., for EOFB).

encryptedSessionKey holds the ciphertext of the encrypted raw session key.

encryptedSaltingKey holds the ciphertext of the encrypted raw media salting key, if any. The salting key is necessary for the enhanced OFB mode.

clearSaltingKey may hold the unencrypted raw media salting key. Implementations shall ascertain that **encryptedSaltingKey** and **clearSaltingKey** shall not be used simultaneously.

paramSsalt holds the initial value for encrypting the salting key. **ClearSalt** optionally holds an unencrypted salting key for salting key encryption (e.g., for EOFB).

NOTE 2 – **generalID**, **algorithmOID** and **paramS** are always transmitted in plaintext, whereas **encryptedSessionKey**, **encryptedSaltingKey** hold the ciphertext of the encrypted key material.

The master generates the key(s) according to the negotiated terminal capabilities and sends the key(s) using **V3KeySyncMaterial** to the peer end point(s). Thus, **V3KeySyncMaterial** shall be forwarded unchanged by intermediate gatekeepers when present.

H.235 version 3 or higher endpoints should always use **secureSharedSecret** within **H235Key** but, depending on the outcome of the logical signalling procedure in 8.2, using the indicating version 3 **ClearToken**, may use **sharedSecret** for backwards compatibility with H.235 version 1 or with version 2 end points.

8.4 Enhanced OFB mode

OFB mode (ISO/IEC 10116) defines an operation mode that deploys a stream cipher using block encryption algorithms. The OFB mode provides:

- improved performance through reduced encryption processing delay;
- easier and less complex handling of incomplete blocks;
- good error resiliency against bit errors.

Enhanced OFB mode is a slightly modified OFB mode called herein "enhanced Output Feedback" mode (EOFB) that deploys the same features as OFB but in addition to that:

1) uses a salting key KS in addition to the encryption key KE; and
2) introduces an implicit packet index.

Usage of an additional secret salting key KS that is being XORed to the feedback yields additional security against known-plaintext analysis. This is a major security benefit that other standard operation (such as CBC, OFB, etc.) modes do not provide. Usage of the EOFB mode would thus yield increased security strength against high-redundancy plaintexts and also against known-plaintext analysis.

EOFB is defined as $C_i = P_i \oplus S_i$ with $S_i = E_{KE}(KS \oplus S_{i-1})$ for $i = 1 \ldots n$ and $S_0 = IV$ where C_i is the i-th ciphertext block, P_i the i-th plaintext block, S_i the i-th key stream block, KE the encryption key and $\oplus$ bitwise XOR. EOFB is illustrated in Figure I.6.

EOFB may also run in standard OFB mode, making EOFB backwards compatible with OFB. In those cases where backwards compatibility with standard OFB mode is desired, the salting key KS shall be either set to all zeroes or equally, leaving **encryptedSaltingKey** within **V3KeySyncMaterial** empty. However, usage of an actual salting key is highly recommended for those cases when encrypting RTP payloads with a block cipher that has a shorter block size such as DES-56 or RC2-compatible.

After at most 2^{48} packets have been processed, a new session encryption key KE and a new salting key KS shall be used, otherwise key stream reuse would occur, thereby compromising the security.

Clause 11 defines object identifiers for DES-56-EOFB, RC2-compatible-EOFB, 3-DES-EOFB and AES-EOFB.

8.5 Key management

Endpoints conforming to this Recommendation should use the fast connect procedure according to 7.6.1. If fast start is not applied, then H.245 tunnelling shall be used to secure the H.245 call control messages by this Recommendation. The fast start procedures allow the establishment of either one or two unidirectional logical channels. The fast start procedure cares for negotiation of the security capabilities, for distribution of a common shared secret (shared DH secret) which acts as a master key, and for secure distribution of an encryption key.

Table 4 provides the allocated OIDs for the various encryption algorithms and relates them with the allocated OIDs for the Diffie-Hellman group. Three D-H groups are identified through an OID:

- "DHdummy": An instance of this DH group should be applied whenever exportable (512 bits) security is of concern or any or non-standard DH group is being used.

  NOTE 1 – No particular DH group is defined; the OID references any non-standard DH group.
- An instance of a 512-bit DH group shall be used to generate a master key for distribution of session key(s) for RC2-compatible ("X") or for DES-56 bit encryption algorithms ("Y").
- "DH1024": This DH group is to be applied when high (1024 bits) security is of concern. The OID references a standardized, fixed DH group. This DH group shall be used to generate a master key for distribution of session key(s) for Triple-DES ("Z") encryption algorithms.
- "DH1536": This DH group is offered as an option for version 3 endpoints having very high security requirements that exceed the security of a 1024-bit DH group. The OID references a fixed DH group. This DH group shall be used to generate a master key for distribution of session key(s) for Triple-DES ("Z", "Z1") or for AES-128 ("Z2", "Z3") encryption algorithms.

It is recommended to apply the defined 1024- or optionally, 1536-bit DH groups unless other security needs would make other Diffie-Hellman parameters preferential. Further, it is recommended to consider using the defined OIDs identifying the DH groups, see 7.8. Nevertheless, implementations should be prepared to obtain the DH group parameters literally without explicit OID indication. In this case, implementations should ascertain that the correct DH group is being conveyed according to Table 4.

Endpoints may use non-standard DH group parameters. Using OID "DHdummy" should indicate such non-standard DH groups. It is left to the decision of the callee whether to accept such DH groups.

NOTE 2 – The choice of the DH group does not eliminate the need to negotiate the actual media encryption algorithm. This shall be accomplished with the H.245 Terminal capability negotiation procedure.

NOTE 3 – During connection establishment (SETUP-to-CONNECT) usage of the encryption algorithm OIDs shall not be used to indicate a Diffie-Hellman instance.

Table 4/H.235.6 – Diffie-Hellman groups

Encryption Algorithm OID	DH-OID	D-H group description
"X", "X1" (RC2-compatible), "Y", "Y1" (DES)	"DHdummy"	Mod-P, any suitable 512-bit prime
"Z", "Z1" (triple-DES), "Z2", "Z3" (AES)	"DH1024"	Mod-P, 1024-bit prime Prime = $2^{1024} – 2^{960} – 1 + 2^{64} × \{ [2^{894}$ pi] + 129093 } = (179769313486231590770839156793787453197860296048756011706444423684197180216158519368947833795864925541502180565485980503646440548199239100050792877003355816639229553136239076508735759914822574862575007425302077447712589550957937778424442426617334727629299387668709205606050270810842907692932019128194467627007)$_{10}$ Generator (Note) = 2
"Z", "Z1" (triple-DES), "Z2", "Z3" (AES)	"DH1536"	Mod-P, 1536-bit prime Prime = $2^{1536} – 2^{1472} – 1 + 2^{64} × \{ [2^{1406}$ pi] + 741804 } = (2410312426921032588552076022197566074856950548502459942654116941958108831682612228890093858261341614673227141477904012196503648957050582631942730706805009223062734745341073406696246014589361659774041027169249453200378729434170325843778659198143763193776859869524088940195577346119843545301547043747207749969763750084308926339295559968882457872412993810129130294592999947926365264059284647209730384947211681434464714438488520940127459844288859336526896320919633919)$_{10}$ Generator (Note) = 2
NOTE – The generator is used to generate the DH token.		

8.6 Key update and synchronization

For 64-bit block ciphers, the key refresh rate *shall* be such that no more than 2^{32} blocks are encrypted using the same key. Implementations *should* refresh keys before 2^{30} blocks have been encrypted using the same key (see 9.1). For 128-bit block ciphers, the key refresh rate *shall* be such that no more than 2^{64} blocks are encrypted using the same key. Implementations *should* refresh keys before 2^{62} blocks have been encrypted using the same key (see 9.1). Both involved entities are free to change the media session key as often as considered necessary due to their security policy. For example, the master may distribute a new session key using **encryptionUpdate** or **encryptionUpdateCommand** of the **miscellaneousCommand** message. On the other hand, the slave can request a new session key from the master by using the **encryptionUpdateRequest** of the **miscellaneousCommand** message.

The **MiscellaneousCommand** message contains the **encryptionUpdate** and **encryptionUpdateCommand** of which the **encryptionSynch** is set with the following parameters:

- **synchFlag**: the new dynamic RTP payload number indicating key changeover.
- **h235key**: carrying the new encrypted session key. This is an H.235 ASN.1 encoded **H235Key** passed as an octet string.

The **sharedSecret** field within the **H235Key** structure uses the following fields:

- **algorithmOID**: set to "X", "X1" for the 56-bit RC2-compatible, set to "Y", "Y1" for 56-bit DES or set to "Z", "Z1" for 168-bit Triple-DES or set to "Z3" for 128-bit AES.

  NOTE 1 – The session key encryption algorithm is the same as the negotiated media encryption algorithm.
- **paramS**: set to the initial value. For 64-bit block stream ciphers, **iv8** holds a random 64-bit block bit pattern that the initiator generates. For 128-bit block stream ciphers, **iv16** holds a random 128-bit block bit pattern that the initiator generates. This field shall not be used for the CBC mode and shall be set to NULL, meaning that the CBC-IV for session key encryption shall be set to 0; it shall only be used for carrying the IV for EOFB mode.
- **encryptedData**: set to the result of the encrypted **KeySyncMaterial**.

As part of the **KeySyncMaterial**:

- **generalID**: identifier of the source distributing the key.

  NOTE 2 – This Recommendation assumes that each endpoint has registered with a gatekeeper and has obtained an endpoint identifier that can be conveyed within **generalID**. This Recommendation does not support scenarios without gatekeepers; this remains for further study.
- **keyMaterial**: set to the new session key. For DES and RC2-compatible this is a 56-bit key, for Triple-DES this is a 168-bit key and for AES this is a 128-bit key. The master shall generate a new session key that meets at least the following security criteria: it is not a weak or semi-weak DES-key and uses a sufficiently secure random source.

The **MiscellaneousCommand** message contains the **encryptionUpdateRequest** that contains **keyProtectionMethod** where the flag **sharedSecret** is set to TRUE.

NOTE 3 – Since the key update and synchronization relies on H.245 messages that are not piggy-backed during fast connect, this requires H.245 tunnelling to be used for secured H.323 entities.

Media session keys do not live forever. At some point in time, each session key expires. A new session key should be used then for protecting an ongoing security session. In conferencing environments, a new group session key should be defined and distributed when group members join or leave a secured conference, thereby preventing them from accessing past or future data.

- Payload-type-based key update and synchronization defines a new dynamic payload type for that new session key; see clauses 8.6.1, 8.6.2 and 8.6.3.

For key update, this Recommendation offers an unacknowledged handshake that is applicable also for H.235 version 1 and version 2 endpoints and also a robust, acknowledged handshake for H.235 version 3 and higher endpoints.

8.6.1 Unacknowledged key update

Figure 4 shows the unacknowledged handshake for session key distribution/key update. If the slave desires an updated session key, the slave may request a new session key from the master by issuing an **encryptionUpdateRequest** to the master. The master shall send a new session key (with or without prior **encryptionUpdateRequest** from the slave) to the slave within an **EncryptionUpdate** message.

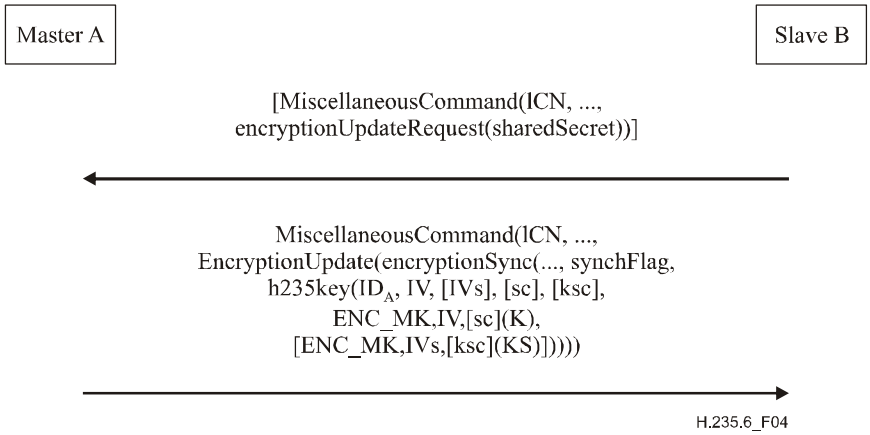


Figure 4/H.235.6 – Unacknowledged session key distribution/key update from the master to the slave(s)

where:

lCN	is the logical channel number;
synchFlag	is the new dynamic RTP payload number;
ID_A	is the **generalID** of the source;
IV	is the initial value/vector for encryption of the sessionkey;
IVs	is the initial value/vector for encryption of the salting key;
ENC_M,IV,sc(K)	means encryption of plaintext *K* using key *M*, initial vector *IV* [and a salting key *sc*, only for EOFB];
KS	is the salting key for the media (for EOFB mode only);
K	is the plaintext session key;
sc	is the unencrypted salting key when EOFB mode is being used for encrypting the session key;
ksc	is the unencrypted salting key when EOFB mode is being used for encrypting the salting key;
s2M/m2S	is the **direction** flag (H.235 v3 and higher only) (s2m = slave-to-master, m2s = master-to-slave);
[]	represents an optional part.

The key update methods as described in the following clauses may deploy EOFB encryption mode for protecting the transmitted key material. In order to deploy EOFB mode for protection of the key material in the same manner as for protection of the media payload, an additional salting key (sc or ksc) is to be used.

8.6.2 Improved key update

H.235 version 3 and higher endpoints shall perform an explicit/implicit acknowledged key update procedure. This is to provide reliable key update methods that are based upon the unacknowledged key update method as provided by pre-H.235v3-based versions. The capability for such procedure shall be negotiated using the version 3 feature indication according to 8.2.

Figure 5 shows the key update procedures for a logical channel owned by the slave. In case the slave initiates the key update and requests a new session key from the master, the slave shall send a **MiscellaneousCommand** to the master where **logicalChannelNumber** shall hold the logical channel number (as defined by the slave), **sharedSecret** shall be set to true, the **direction** flag shall be set to **slaveToMaster** and the new dynamic payload number shall be requested in **synchFlag** within **EncryptionUpdateRequest**. If, otherwise, the master initiates the key update, this **EncryptionUpdateRequest** message shall not be sent.

The master, either responding to the slave's request or on its own behalf, shall issue an **EncryptionUpdateCommand** where the **logicalChannelNumber** shall hold the logical channel number, **direction** shall be set to **slaveToMaster** within **MiscellaneousCommand** and **synchFlag** within **encryptionSync** reflects the new dynamic payload number.

h235key shall carry the new session key. **h235key** shall hold the identity of the master in **generalID** and the applied initial vector *IV* in **paramS**. The encrypted media session key shall be conveyed within **encryptedSessionKey**, where the encryption function shall apply the master session key and the initial value in **paramS** to the session key *K***.** For EOFB, an unencrypted salting key is conveyed in **ClearSalt** within **paramS** (*sc*). **encryptedSaltingKey** shall convey the encrypted media salting key, where the encryption function shall apply the master session key and the initial value **paramSsaltIV** to the media salting key *KS*. For EOFB, an unencrypted salting key (*ksc*) is conveyed in **ClearSalt** within **paramSsalt**. **clearSaltingKey** may hold an unencrypted media salting key in which case, **encryptedSaltingKey** shall remain empty and vice versa. The transmission of an unencrypted salting key shall only be achieved if the security does not suffer, in any other case, it is recommended that the media salting key be encrypted.

The master shall be prepared to receive encrypted media under the new session key upon submitting the **EncryptionUpdateCommand** but should continue using the old session key until reception of the **EncryptionUpdateAck**. The master may apply the new session beginning with reception of the **encryptionUpdateAck**, while the slave may apply the new session key beginning with reception of the **EncryptionUpdateCommand**.

NOTE 1 – The master may choose any dynamic payload type value for the slave since the payload type is just tied to the port of the media channel.

NOTE 2 – There is no need for the slave to explicitly acknowledge reception of the new key. The master is able to deduce the reception of the issued key by the slave, when receiving media encrypted under the new payload type.

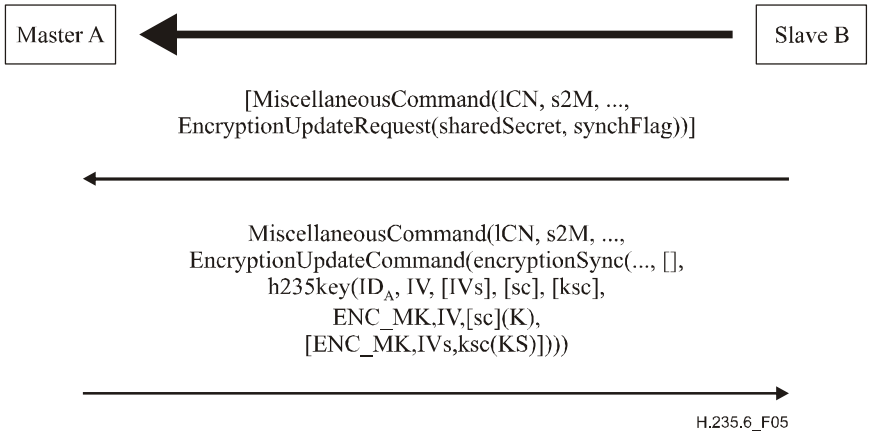


Figure 5/H.235.6 – Session key update on slave's logical channel

Figure 6 shows the key update procedures for a logical channel owned by the master. In case the slave initiates the key update and requests a new session key from the master, the slave shall send a **MiscellaneousCommand** to the master where **logicalChannelNumber** shall hold the logical channel number (as defined by the master), **sharedSecret** shall be set to true, the **direction** flag shall be set to **masterToSlave**. If, otherwise, the master initiates the key update, this **EncryptionUpdateRequest** message shall not be sent.

The master, either responding to the slave's request or on its own behalf, shall issue an **EncryptionUpdateCommand** where the **logicalChannelNumber** shall hold the logical channel number, **direction** shall be set to **masterToSlave**, **encryptionSync** shall provide the **synchFlag** with the new dynamic payload number. **h235key** shall carry the new session key. **h235key** shall hold the identity of the master in **generalID** and the applied initial vector *IV* in **paramS**. The encrypted media session key shall be conveyed within **encryptedSessionKey**, where the encryption function shall apply the master key and the initial value in **paramS** to the session key *K*. For EOFB, an unencrypted salting key is conveyed in **ClearSalt** within **paramS** (*sc*). For EOFB,

encryptedSaltingKey shall convey the encrypted media salting key, where the encryption function shall apply the master session key and the initial value **paramSsaltIV** to the salting key *KS*. For EOFB, an unencrypted salting key (*ksc*) is conveyed in **ClearSalt** within **paramSsalt**. **clearSaltingKey** may hold an unencrypted media salting key in which case **encryptedSaltingKey** shall remain empty and vice versa. The transmission of an unencrypted salting key shall only be achieved if the security does not suffer, in any other case, it is recommended that the media salting key be encrypted.

The slave shall acknowledge reception of the new session key by responding with **MiscellaneousCommand** where the **logicalChannelNumber** shall hold the logical channel number, and **encryptionUpdateAck** shall reflect the new dynamic payload number in **synchFlag**.

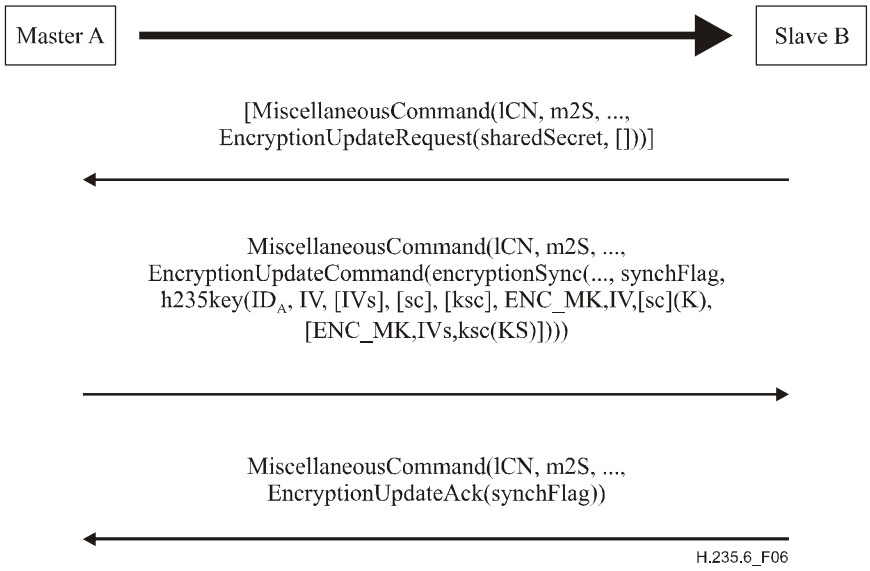


Figure 6/H.235.6 – Session key update on master's logical channel

8.6.3 Payload-type-based key update and synchronization

Initial encryption key is presented by the master in conjunction with the dynamic payload number in **synchFlag** (via **EncryptionSync** in ITU-T Rec. H.245). The receiver(s) of the media stream shall start initial use of the key upon receipt of this payload number in the RTP header.

If the negotiated logical channel carries only a single payload type, the value of the **synchFlag** may replace the negotiated payload type in the RTP header. If, on the other hand, the negotiated logical channel may carry more than one payload type (even if only in separate RTP packets), then the RTP packets shall be formatted as described in RFC 2198, with the **synchFlag** value acting as the encapsulating payload type, and the actual payload type(s) residing in the additional header block(s) as specified by RFC 2198.

New key(s) may be distributed at any time by the master endpoint. The synchronization of the newer key with the media stream shall be indicated by the changing of the payload type to a new dynamic value.

NOTE – The specific values do not matter, as long as they change for every new key that is distributed.

8.7 Non-terminal interactions

8.7.1 Gateway

As stated in 6.6/H.235.0, an H.323 gateway should be considered a trusted element. This includes protocol gateways (H.323-H.320 etc.) and security gateways (proxy/firewalls). The media privacy

can be assured between the communicating endpoint and the gateway device; but what occurs on the far side of the gateway should be considered insecure by default.

8.7.2 New keys

The procedures outlined in 8.5/H.323 are completed by an MC to eject a participant from a conference. The master may generate new encryption keys for the logical channels (and not distribute them to the ejected party); this may be used to keep the ejected party from monitoring the media streams.

8.7.3 H.323 trusted elements

In general, MC(U)s, gateways, and gatekeepers (if implementing the gatekeeper-routed model) are trusted with respect to the privacy of the control channel. If the connections establishment channel (H.225.0) is secured *and* routed through the gatekeeper, it must also be trusted. If any of these H.323 components must operate on the media streams (i.e., mixing, transcoding) then, by definition, they shall also be trusted for the media privacy.

Firewall proxies (though not H.323-specific elements) may also be trusted, since they terminate connections, and may well have to manipulate the messages and media streams.

8.8 Multipoint procedures

8.8.1 Authentication

Authentication shall occur between an endpoint and the MC(U) in the same manner that it would in a point-to-point conference. The MC(U) shall set the policy concerning level and stringency of authentication. As stated in 6.6/H.235.0, the MC(U) is trusted; existing endpoints in a conference may be limited by the authentication level employed by the MC(U). New **ConferenceRequest**/**ConferenceResponse** commands allow endpoints to obtain the certificates of other participants in the conference from the MC(U). As outlined in H.245 procedures, endpoints in a multipoint conference may request other endpoint certificates via the MC, but may not be able to perform direct cryptographic authentication within the H.245 channel.

8.8.2 Privacy

MC(U) shall win all master/slave exchanges and, as such, shall supply encryption key(s) to participants in a multipoint conference. Privacy for individual sources within a common session (assuming multicast) may be achieved with individual or common keys. These two modes may be arbitrarily chosen by the MC(U) and shall not be controllable from any particular endpoint except in modes allowed by MC(U) policy. In other words, a common key may be used across multiple logical channels as opened from different sources.

9 Media stream encryption procedures

Media streams shall be encoded using the algorithm and key as presented in the H.245 channel. Figures 7 and 8 show the general flow. Note that the transport header is attached to the transport SDU after the SDU has been encrypted. The opaque segments indicate privacy. As new keys are received by the transmitter and used in the encryption, the SDU header shall indicate in some manner to the receiver that the new key is now in use. For example, in ITU-T Rec. H.323, the RTP header (SDU) will change its payload type to indicate the switch to the new key.

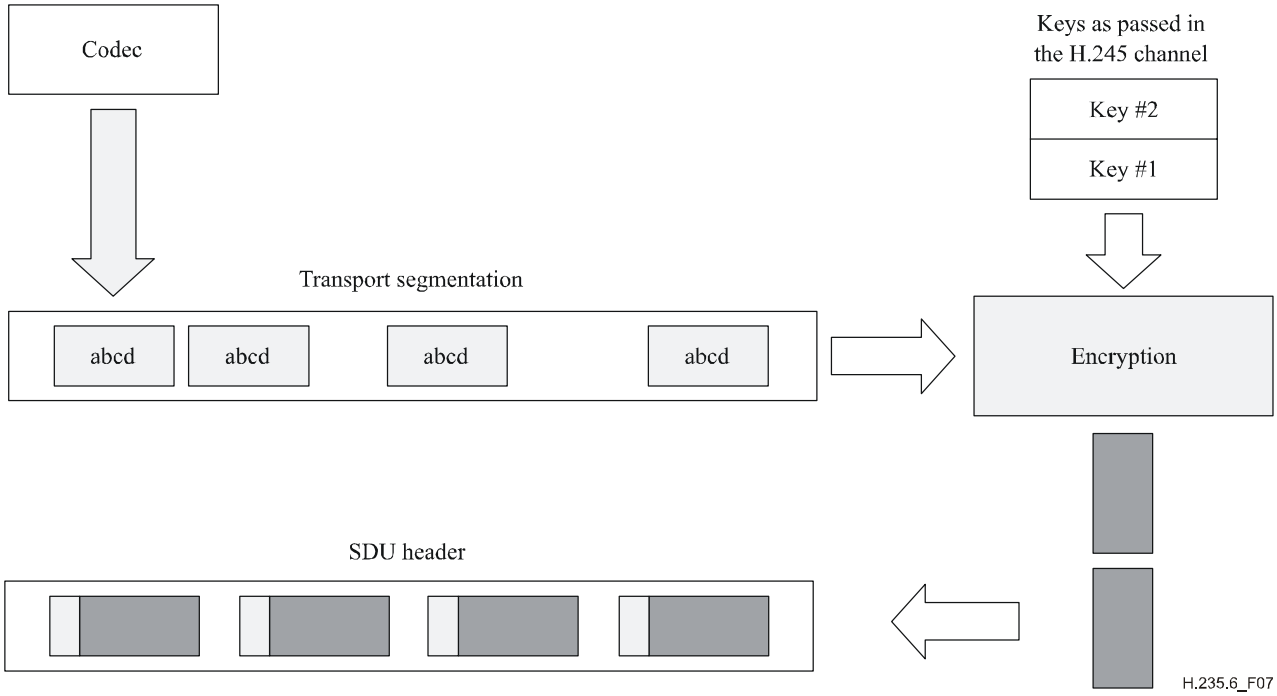


Figure 7/H.235.6 – Encryption of media

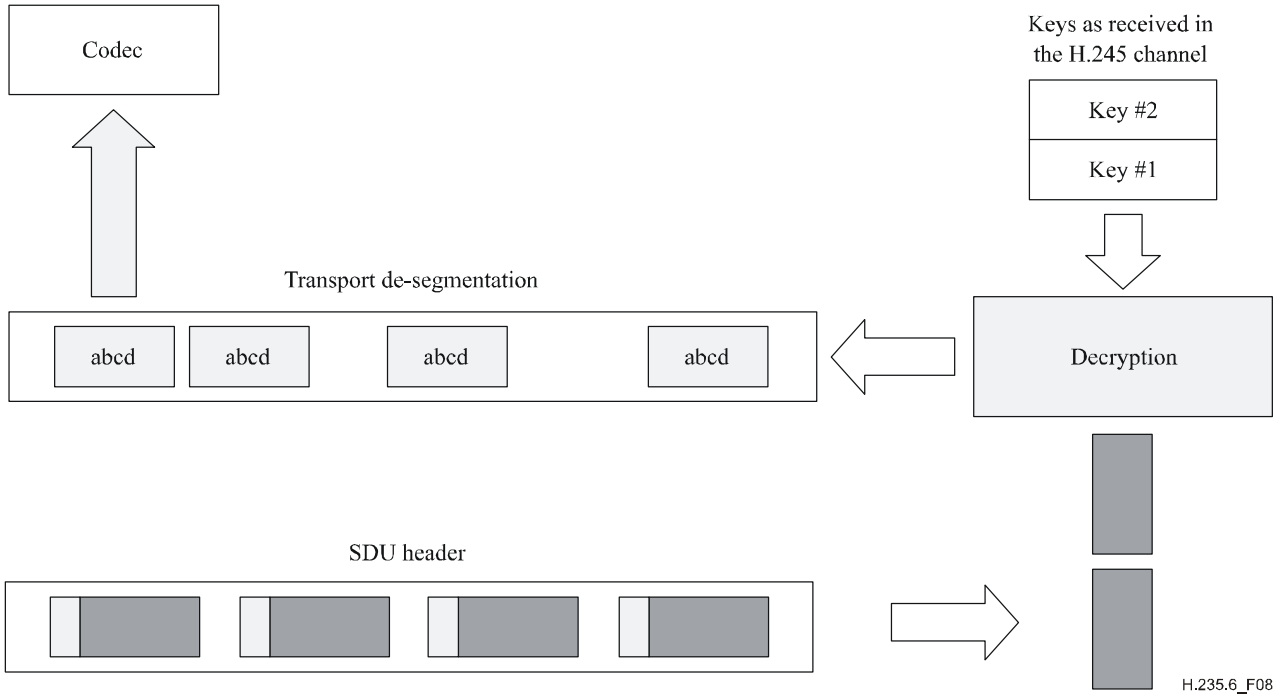


Figure 8/H.235.6 – Decryption of media

9.1 Media session keys

Included in the **encryptionUpdate** is the **h235Key**. The **h235Key** is ASN.1 encoded within the context of the H.235 ASN.1 tree, and passed as an opaque octet string with respect to H.245. The key may be protected by utilizing one of the three possible mechanisms as they are passed between two endpoints.

- If the H.245 channel is secure, no additional protection is applied to the key material. The key is passed "in the clear" with respect to this field; the ASN.1 choice of **secureChannel** is utilized.
- If a secret key and algorithm has been established outside the H.245 channel as a whole (i.e., outside H.323 or on an **h235Control** logical channel), the shared secret is used to encrypt the key material; the resultant enciphered key is included here. In this case, the ASN.1 choice of **sharedSecret** is used.
- Certificates may be used when the H.245 channel is not secure, but may also be used in addition to the secure H.245 channel. When certificates are utilized, the key material is enciphered using the certificate's public key and the ASN.1 construct **certProtectedKey**.

At any point in a conference, a receiver (or transmitter) may request a new key (**encryptionUpdateRequest**). One reason it might do this is if it suspects that it has lost synchronization of one of the logical channels. The master receiving this request shall generate new key(s) in response to this command. The master may also decide asynchronously to distribute new key(s), if so, it shall use the **encryptionUpdate** message.

After receiving an **encryptionUpdateRequest**, a master shall send out **encryptionUpdate**. If the conference is a multipoint one, the MC (also the master) should distribute the new key to all receivers before it gives this key to the transmitter. The transmitter of the data on the logical channel shall utilize the new key at the earliest possible time after receiving the message.

A transmitter (assuming it is not the master) may also request a new key. If the transmitter is part of a multipoint conference, the procedure shall be as follows:

- The transmitter shall send the **encryptionUpdateRequest** to the MC (master).
- The MC should generate a new key(s) and send an **encryptionUpdate** message to all conference participants except the transmitter.
- After distributing the new keys to all other participants, the MC shall send the **encryptionUpdate** to the transmitter. The transmitter shall then utilize the new key.

9.2 Media anti-spamming

The receiver of an RTP media stream may wish to counter denial-of-service and flooding attacks on discovered RTP/UDP ports. Receivers, when having implemented the anti-spam capability, can quickly determine whether an obtained RTP packet stems from an unauthorized source and discard it.

The anti-spamming capability, when set, indicates use of the anti-spamming mechanism either:

- for plaintext media data without media encryption (see case 1 below); or
- in combination with encrypted media data when **EncryptionCapability** features an encryption algorithm (see case 2 below).

Both options provide a lightweight **RTP packet authentication** on selected fields through a computed message authentication code (MAC). The MAC may be computed using the object identifiers defined in 9.2.1. The cryptographic algorithms are by:

- an encryption algorithm (e.g., DES in MAC mode see ISO/IEC 9797-1 and 9797-2). DES-MAC is indicated using the OID "N" while triple-DES-MAC is indicated using OID "O"; or
- using a cryptographic one-way function (e.g., SHA1). The OID to be used is "M".

The MAC algorithm is indicated in the object identifier of **antiSpamAlgorithm**. The algorithm OID implicitly indicates also the size of the MAC; e.g., 1 block = 64 bits for DES MAC. In order to save bandwidth, the MAC could be truncated, albeit sacrificing some security, e.g., to a 32-bit

MAC; this then requires a different object identifier. The anti-spam method is independent of any additional payload encryption (see cases 1 and 2 below).

Anti-spamming uses the following RTP packet format (see Figure 9) where the RTP padding sequence is interpreted as follows (see clause 5 in RFC 3550).

- The P bit in the RTP header shall be set to 1.
- Padding bytes shall be appended at the end of the payload with the following meaning:

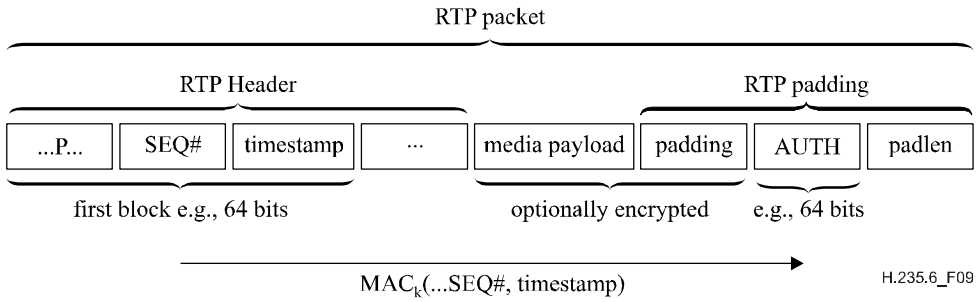


Figure 9/H.235.6 – RTP packet format for media anti-spamming

NOTE 1 – If anti-spamming is not used, then the AUTH and padlen fields are not used either and the usual RTP packet format applies.

1) *Case anti-spamming-only*

This case applies when the media data are not encrypted and the padding fields are left empty. The last octet of the RTP padding contains a count of how many padding octets should be ignored at the end of the RTP packet. The other padding bytes carry the MAC. The MAC shall be computed over the first crypto block of the RTP header including the varying timestamp and sequence number using the negotiated MAC algorithm of **antiSpamAlgorithm** and applying the symmetric secret. A static or manually configured shared secret, or a dynamically negotiated shared secret *k* may be used according to the procedures of ITU-T Rec. H.235.0. For larger block sizes (more than 64 bits), some sufficient additional bits of the RTP header, or even the first media payload, shall be taken.

For the MAC computation, it is recommended to use the key that is obtained from the H.235 media session key distribution; although the session key applied is not used for payload encryption. Secure fast connect with key establishment (see Annex J/H.323) or manual keying may be used for key management. The sender computes the MAC as described above and includes the result in the MAC field in the RTP padding AUTH field. Sender and receiver know the size of the AUTH field and the length of the MAC by the **antiSpamAlgorithm**.

The MAC verification at the receiver side should be done as early as possible, if possible already within the RTP stack, or at latest, before decryption or decompressing the payload. The receiver first recomputes the MAC in the same way as the sender did and compares the computed MAC with the delivered MAC in the RTP padding. If the MACs do not match, the RTP header has been modified in transit or was sent by an unauthorized entity that does not possess the key. Thus, the mis-authenticated RTP packet shall be discarded, the event may be logged; this indicates a probable attempt of denial-of-service attack. Otherwise, the authenticated RTP packet can be processed further, the RTP padding is removed and the payload is fed through the codec.

NOTE 2 – The lightweight MAC computation/verification with DES encryption involves only a single encryption operation; alternatively, SHA1 MAC is computed on a short part of the packets of fixed length, thus the crypto operations consume absolutely minimal processing resources.

2) *Case anti-spam method and payload encryption*

This case applies when the media data are encrypted and the anti-spamming method is invoked. When the payload does not fall on even block boundaries, some additional padding bytes have to be appended to the payload in front of the MAC. The media payload encryption is according to this clause 9.

EncryptionCapability defines the payload encryption algorithm while **antiSpamAlgorithm** defines the anti-spamming method. For security reasons, the media encryption and the MAC shall use different session keys. The MAC key *k* is computed by feeding the encryption key *K* through the SHA1 one-way hash function;

k = SHA1(*K*); sufficient bits shall be taken from the hashed result in network byte order. When **antiSpamAlgorithm** indicates an encryption algorithm, then the collected bits shall be made a correct encryption key; e.g., setting DES parity bits.

After the receiver successfully verifies the authenticity of the RTP packet, the payload is decrypted and the RTP padding is then discarded. The general procedure is according to case 1 above.

9.2.1 List of object identifiers

Table 5 lists all the referenced OIDs.

Table 5/H.235.6 – Object identifiers used for anti-spamming

Object identifier reference	Object identifier value	Description
"M"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 8}	anti-spamming using HMAC-SHA1-96
"N"	{iso(1) identified-organization(3) oiw(14), secsig(3) algorithm(2) desMAC(10)}	anti-spamming using DES (56 bits) MAC (see ISO/IEC 9797-1 and 9797-2) with 64-bit MAC
"O"	{iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) desEDE(17)}	anti-spamming using triple-DES (168-bits) MAC (see ISO/IEC 9797-1 and 9797-2)

9.3 RTP/RTCP issues

The use of encryption on the RTP stream will follow the general methodology recommended in the document referenced in [RTP]. The encryption of the media shall occur in an independent, packet-by-packet basis.

NOTE – It should be noted that if RTP packet size is larger than MTU size, partial loss (of fragment) will cause the whole RTP packet to be indecipherable

The RTP header shall not be encrypted. For audio/video codecs, the entire audio/video codec payload including any audio/video payload header(s) shall be encrypted. Synchronization of new keys and encrypted text is based upon dynamic payload type (see 8.6.3).

It is assumed that encryption is applied just to the payload in each RTP packet, the RTP headers remaining in the clear. It is assumed that all RTP packets must be a multiple of whole octets. How the RTP packets are encapsulated at the transport or network layer is not relevant to this Recommendation. All modes must allow for lost (or out-of-sequence) packets, in addition to padding packets to an appropriate multiple of octets.

Deciphering the stream must be stateless due to the fact that packets may be lost; each packet should be deciphered independently. Two requirements of block algorithm mode shall operate as follows:

9.3.1 Initialization vectors

Most block modes involve some "chaining"; each encryption cycle depends in some way on the output of the previous cycle. Therefore, at the beginning of a packet, some initial block value (usually called an Initialization Vector (IV)) must be provided in order to start the encryption process. Independent of how many stream octets are processed on each encryption cycle, the length of the IV is always equal to the length of a block. All modes except Electronic Code Book (ECB) mode require an IV.

9.3.1.1 CBC initialization vector

An Initialization Vector (IV) is required when using a block cipher in CBC mode to encrypt RTP packet payloads. The size of an IV is the same as the block size for the particular block cipher. For example, the IV size for DES and 3-DES is 64 bits, while for AES it is 128 bits.

For the CBC case, an IV shall be constructed from the first *B* (where *B* is the block size) octets of: Seq# concatenated with Timestamp. This forms the pattern, *SSTTTT*, where *SS* is the 2-octet RTP Seq# and *TTTT* is the 4-octet RTP timestamp. This pattern shall be repeated until *B* octets have been generated, truncating as necessary. For example, 64- and 128-bit IVs would contain *SSTTTTSS* and *SSTTTTSSTTTTSSTT*, respectively. It should be noted that the IV generated in this manner may produce a key pattern that is considered "weak" for a particular algorithm.

9.3.1.2 EOFB initialization vector

The unique initial vector IV for each RTP packet in EOFB mode shall be computed as follows:

Each RTP packet is associated with an implicit 48-bit packet index *i* as defined in [SRTP] where $i = 2^{16} \times \text{ROC} + \text{SEQ}$ with SEQ the sequence number taken from the RTP header and ROC is the 32-bit rollover counter counting how often the sequence number SEQ has been wrapped around through 65535.

Initially, the rollover counter ROC shall be set to zero. Each time the SEQ wraps modulo 2^{16}, the sender shall increment ROC by one modulo 2^{32}.

The initial vector IV is computed as ($i \parallel T$ [$\parallel i \parallel T \parallel$ ...]) with the 48-bit index *i* and 32-bit timestamp *T* taken from the RTP header concatenated several times until the block size is filled-up. The $\parallel$ symbol represents concatenation.

NOTE – The rollover counter and IV are maintained and computed locally at each peer side and do not get transmitted.

The receiver, when facing lost or reordered packets, should compute an estimated index *i* as:

$i = 2^{16} \times v + \text{SEQ}$ where *v* is chosen from the set {ROC-1, ROC, ROC+1} modulo 2^{32} such that *v* is closest (in 2^{48} sense) to the value $2^{16} \times \text{ROC} + s_l$ where s_l is the maintained sequence number at the receiver. After the packet has been processed using the estimated index, the receiver shall decide if s_l and ROC should be updated. For instance, a simple (but not error robust) method is to simply set s_l to SEQ (if SEQ > s_l) and, if the value v = ROC + 1 was used, to update ROC to *v*; see also [SRTP], section 3.2.1, for more information.

9.3.2 Padding

ECB and CBC modes always process the input stream a block at a time and, while CFB and OFB can process the input in any number of octets, *N* ($\leq B$), it is recommended that $N = B$.

Two methods are available to handle packets whose payload is not a multiple of blocks:

1) Ciphertext Stealing for incomplete blocks for ECB and CBC; no padding for CFB and EOFB.

2) Padding in the manner prescribed by [RTP], section 5.1.

[RTP], section 5.1 describes a method of padding in which the payload shall be padded to a multiple of blocks. The last octet shall be set to the number of padding octets (including the last), and the *P* bit set in the RTP header. The value of the pad should be determined by the normal convention of the cipher algorithm.

All H.235 implementations shall support both schemes. The scheme in use can be deduced as follows: if the *P* bit is set in the RTP header, then the packet is padded; if the packet is not a multiple of *B* and the *P* bit is not set, then Ciphertext Stealing applies, else the packet is a multiple of B, and padding does not apply.

9.3.3 RTCP protection

Application of cryptographic techniques to RTCP elements is for further study.

9.3.4 Secured payload stream

H.323-based networks, when being used, for example, for Modem-over-IP transmission, deploy H.245 signalling to establish and negotiate a voice band data channel and RTP for packetization of a Multiple Payload Stream (MPS).

For a single media stream with a single payload type or FEC for another channel, the dynamic payload type in **encryptionSync** shall replace the default payload type.

For encapsulating streams, (i.e., redundancy encoding or RFC 2198 encoded FEC) the dynamic payload type within **encryptionSync** shall replace the encapsulating payload type.

For multiple payload streams, the dynamic payload type in **syncflag** of **encryptionSync** shall be ignored and the (optional) payload types within the **multiplePayloadStreamElement**(s) shall be used instead.

The **encryptionUpdateCommand** shall be used for the improved key update procedure to distribute new session key material (see 8.6.2). **multiplePayloadStream** is only used when a multiple payload stream is to be re-keyed, in which case the dynamic payload type within **EncryptionSync** shall be ignored.

9.3.5 Interworking with J.170

For further study.

9.4 Triple-DES in outer CBC mode

168-bit triple-DES in outer CBC mode, as illustrated in Figure 10, s*hould* be used within this security profile. In the figure, each k_i refers to a 56-bit key. A different 56-bit key *shall* be used within each encryption (E) and decryption (D) block. None of the 64 weak keys for DES are known to cause any weakness within triple-DES. However, implementations complying with this profile should reject the key when a weak DES key is involved (see RFC 2405).

More information on triple-DES may be obtained from [Schneier] and [RFC2405].

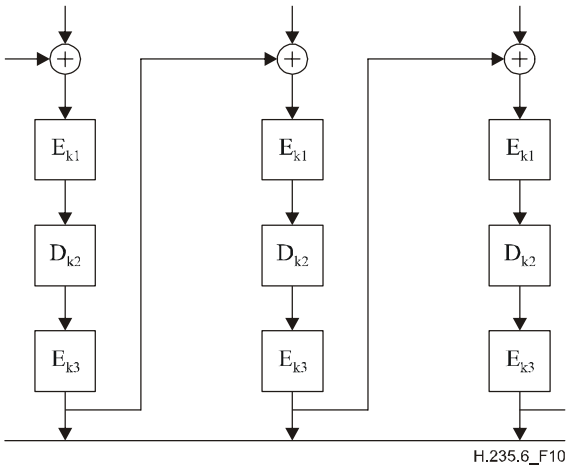


Figure 10/H.235.6 – Triple-DES encryption in outer CBC mode

9.5 DES algorithm operating in EOFB mode

Voice may be encrypted using the DES algorithm operating in the EOFB stream cipher block-chaining mode. EOFB mode allows exploiting parallelism in implementations. When operating in EOFB mode, it is recommended, for both performance and security reasons, to feedback the entire crypto block (i.e., the full 64-bits for DES for example with $n = j = 64$). However, due to the fact that EOFB does not provide chaining across the blocks and bits, EOFB may be susceptible to specific attacks depending on the statistical properties of the input plaintext data. Thus, key updating (see 8.6) should be performed regularly but, at latest, before the initial value wraps around. For the computation of the initial value see 9.3.1.2.

9.6 Triple-DES in outer EOFB mode

168-bit triple-DES in outer EOFB mode, as illustrated in Figure 11, may be used within this security profile. In the figure, each k_i refers to a 56-bit key. A different 56-bit key *shall* be used within each encryption (E) and decryption (D) block. None of the 64 weak keys for DES are known to cause any weakness within triple-DES. However, implementations complying with this profile should reject the key when a weak DES key is involved [RFC2405].

More information on triple-DES may be obtained from [Schneier], [RFC2405].

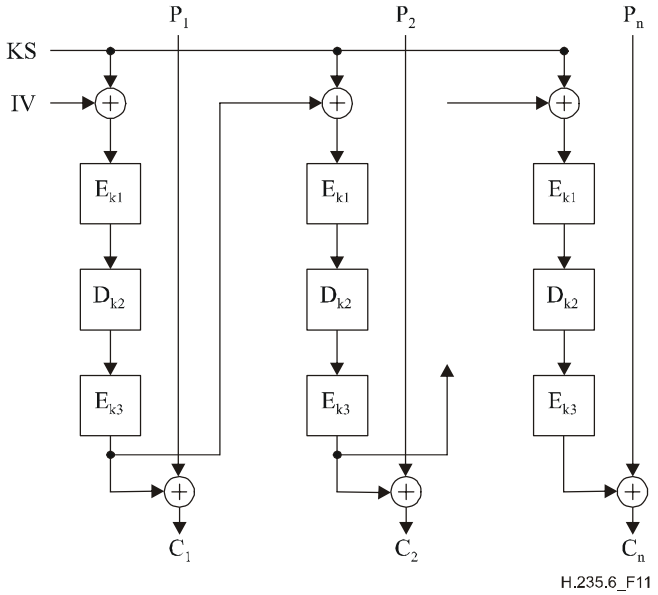


Figure 11/H.235.6 – Triple DES encryption in outer EOFB mode

10 Lawful interception

For further study (see [LI]).

11 List of object identifiers

Table 6 lists all the referenced OIDs (see also [OIW] and [WEBOIDs]). There are object identifiers for H.235v1 (ITU-T Rec. H.235v1) and for H.235v2 (ITU-T Rec. H.235v2).

Table 6/H.235.6 – Object identifiers

Object identifier reference	Object identifier value(s)	Description
"DHdummy"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 40} {itu-t (0) recommendation (0) h (8) 235 version (0) 3 40}	Non-standard DH-group explicitly provided
"DH1024"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 43} {itu-t (0) recommendation (0) h (8) 235 version (0) 3 43}	1024-bit DH group
"DH1536"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 44}	1536-bit DH group
"X"	{iso(1) member-body(2) us(840) rsadsi(113549) encryptionalgorithm(3) 2}	Voice encryption using RC2-compatible (56 bits) or RC2-compatible in CBC mode and 512-bit DH-group.
"X1"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 27}	Voice encryption using RC2-compatible (56 bits) or RC2-compatible in EOFB mode and 512-bit DH-group
"Y"	{iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) descbc(7)}	Voice encryption using DES (56 bits) in CBC mode and 512-bit DH-group.

Table 6/H.235.6 – Object identifiers

Object identifier reference	Object identifier value(s)	Description
"Y1"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 28}	Voice encryption using DES (56 bits) in EOFB mode and 512-bit DH-group with 64-bit feedback
"Z1"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 29}	Voice encryption using Triple-DES (168-bits) in outer-EOFB mode and 1024-bit DH-group with 64-bit feedback
"Z2"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 30}	Voice encryption using AES (128-bits) in EOFB mode and 1024-bit DH-group
"Z3"	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) 3 nistAlgorithm(4) aes(1) cbc(2)}	Voice encryption using AES (128-bits) in CBC mode and 1024-bit DH-group
"Z"	{iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) desEDE(17)}	Voice encryption using triple-DES (168-bits) in outer-CBC mode and 1024-bit DH-group.

Appendix I

H.323 implementation details

I.1 Ciphertext padding methods

There is a description of Ciphertext Stealing in [Schneier], pages 191 and 196. Figures I.1 to I.5 illustrate the technique.

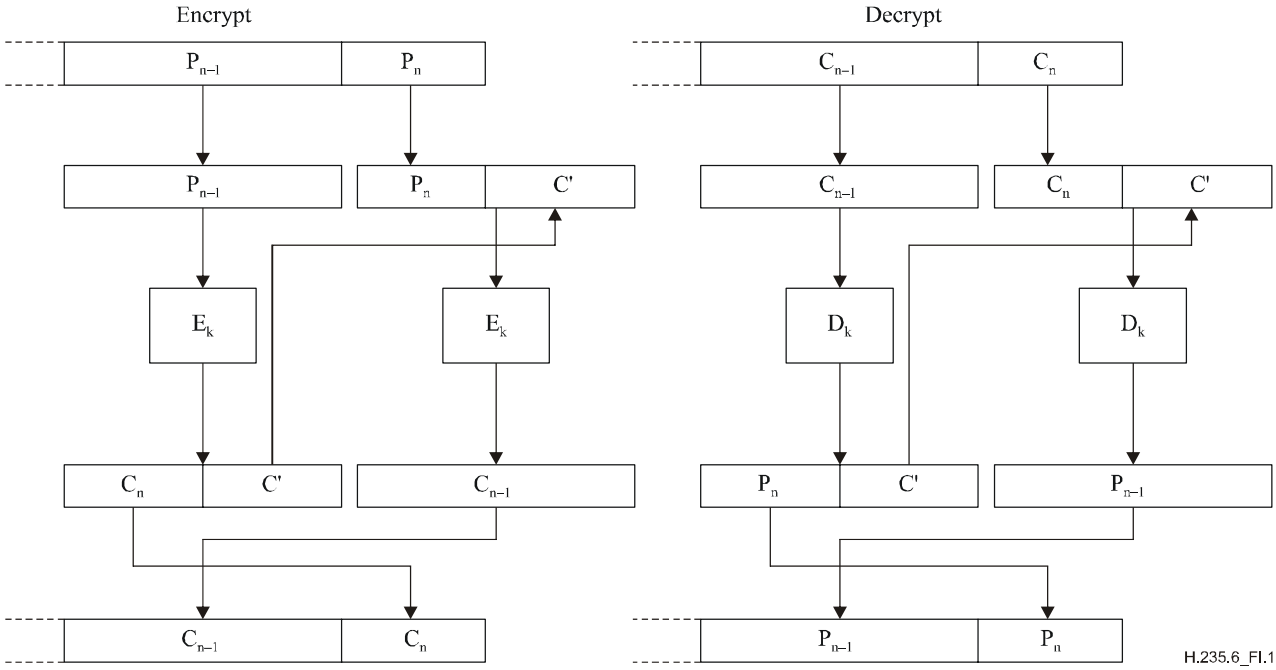


Figure I.1/H.235.6 – Ciphertext stealing in ECB mode

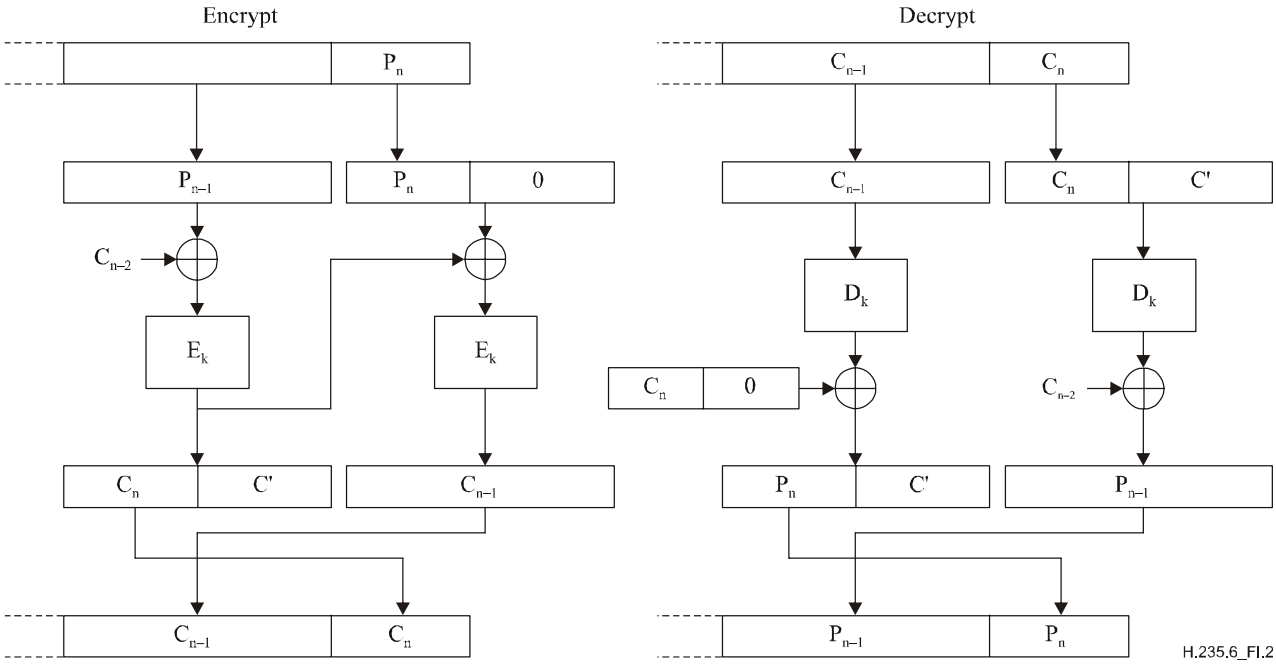


Figure I.2/H.235.6 – Ciphertext stealing in CBC mode

NOTE – Ciphertext stealing in ECB or CBC modes requires the payload to convey at least one complete block. Implementations deploying ciphertext stealing in ECB mode or CBC modes should ascertain that the payload conveys always at least one crypto block; e.g., by proper choice of the sampling/packetization rate or selection of the encryption algorithm.

In case the payload spans less than one single block, the initial vector (IV) shall be used as the previous ciphertext block when ciphertext stealing mode is applied in CBC mode.

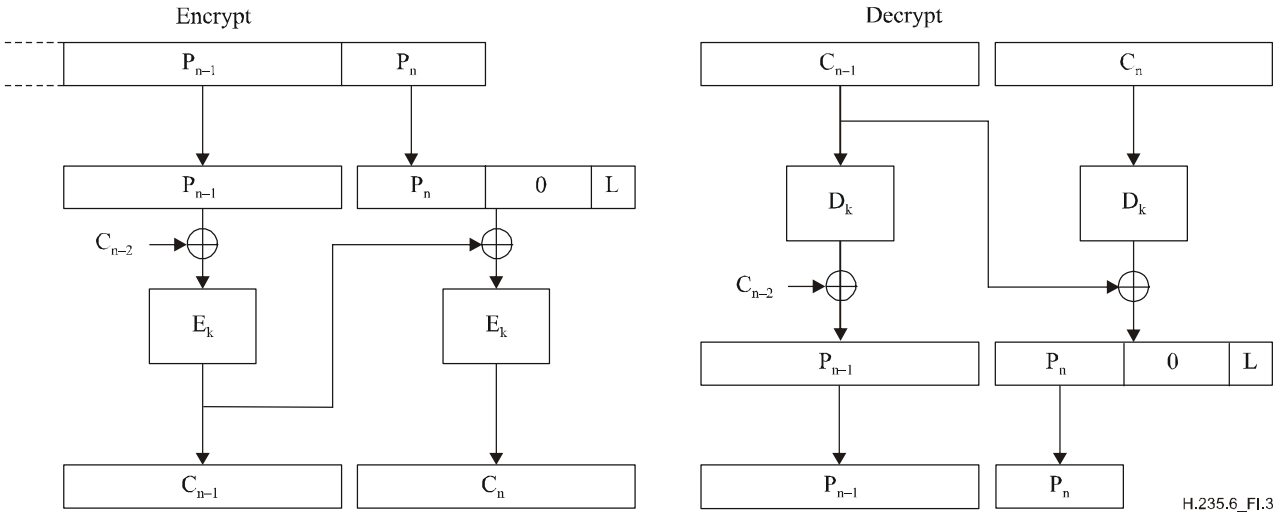


Figure I.3/H.235.6 – Zero padding in CBC mode

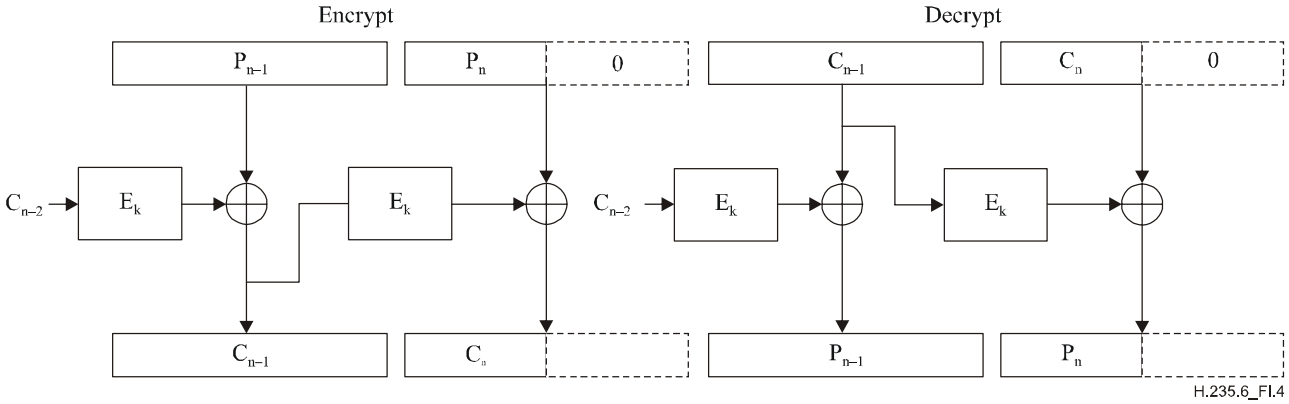
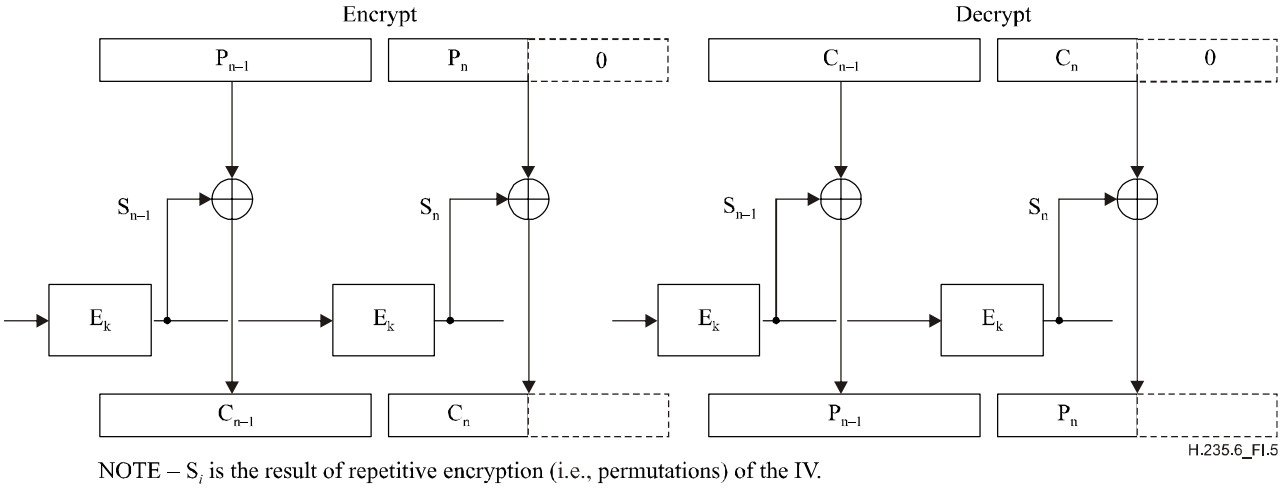


Figure I.4/H.235.6 – Zero padding in CFB mode



NOTE – S_i is the result of repetitive encryption (i.e., permutations) of the IV.

Figure I.5/H.235.6 – Zero padding in OFB mode

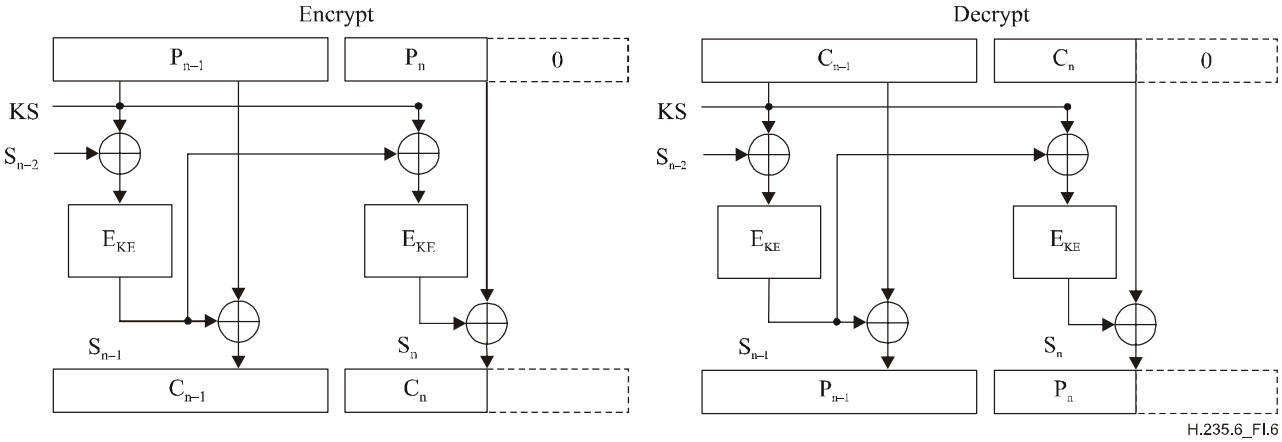


Figure I.6/H.235.6 – EOFB mode with zero padding

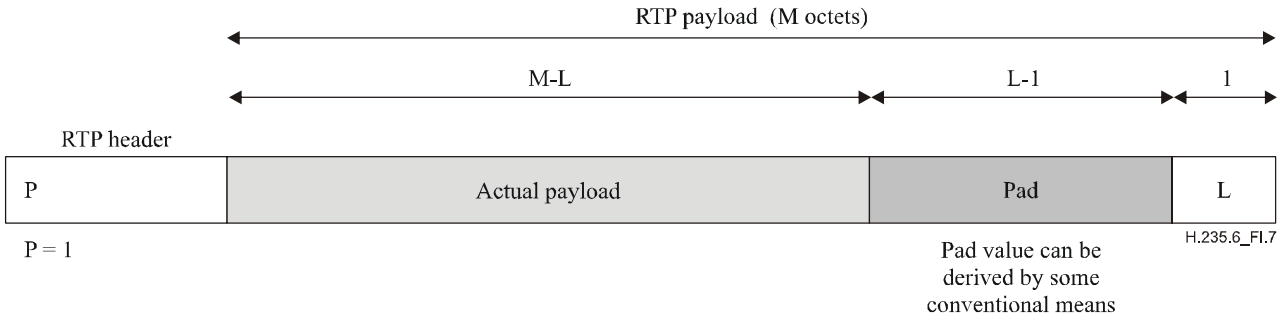


Figure I.7/H.235.6 – Padding as prescribed by RTP

I.2 New keys

The procedures outlined in 8.5/H.323 are completed by an MC to eject a participant from a conference. The master may generate new encryption keys for the logical channels (and not distribute them to the ejected party); this may be used to keep the ejected party from monitoring the media streams.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
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	Telecommunication management, including TMN and network maintenance
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, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2006