

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.235.6

(01/2014)

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

H.323 security: Encryption profile with native ITU-T H.235/H.245 key management

Recommendation ITU-T H.235.6



International
Telecommunication
Union

Document Sharing Hub

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, TRIPLE-PLAY AND ADVANCED MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619
Advanced multimedia services and applications	H.620–H.629
Ubiquitous sensor network applications and Internet of Things	H.640–H.649
IPTV MULTIMEDIA SERVICES AND APPLICATIONS FOR IPTV	
General aspects	H.700–H.719
IPTV terminal devices	H.720–H.729
IPTV middleware	H.730–H.739
IPTV application event handling	H.740–H.749
IPTV metadata	H.750–H.759
IPTV multimedia application frameworks	H.760–H.769
IPTV service discovery up to consumption	H.770–H.779
Digital Signage	H.780–H.789
E-HEALTH MULTIMEDIA SERVICES AND APPLICATIONS	
Interoperability compliance testing of personal health systems (HRN, PAN, LAN and WAN)	H.820–H.849
Multimedia e-health data exchange services	H.860–H.869

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T H.235.6

H.323 security: Encryption profile with native ITU-T H.235/H.245 key management

Summary

Recommendation ITU-T H.235.6 holds the security procedures for the encryption profile (formerly in Annex D of Recommendation ITU-T H.235 version 1) including the accompanying native ITU-T H.235/H.245 key management.

This revision introduces support for key lengths larger than 2048 bits. In previous versions, bit sizes of 3072 and 4096 were defined. However, the field size defined in Recommendation ITU-T H.235.0 was limited to 2048 bits.

Version 4 of Recommendation ITU-T H.235 broke up Recommendation ITU-T H.235 version 3 into a suite of ITU-T H.235.x sub-series Recommendations, and it restructured the sub-series. In earlier versions, prior to version 4 of the ITU-T H.235 sub-series, this profile was contained in the main body and Annex D of Recommendation ITU-T H.235 version 1. Appendices IV, V and VI to Recommendation ITU-T H.235.0 show the complete clause, figure and table mapping between Recommendation ITU-T H.235 versions 3 and 4.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T H.235.6	2005-09-13	16	11.1002/1000/8598-en
1.1	ITU-T H.235.6 (2005) Amd. 1	2008-06-13	16	11.1002/1000/9472-en
2.0	ITU-T H.235.6	2009-03-16	16	11.1002/1000/9694-en
3.0	ITU-T H.235.6	2014-01-13	16	11.1002/1000/12059-en

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). 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, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2014

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

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Terms and definitions	2
4	Abbreviations and acronyms	3
5	Conventions	4
6	System overview.....	4
6.1	Encryption security profile	4
7	ITU-T H.245 signalling and procedures.....	6
7.1	Secure ITU-T H.245 channel operation	6
7.2	Unsecured ITU-T H.245 channel operation	6
7.3	Capability exchange	6
7.4	Master role.....	7
7.5	Logical channel signalling.....	7
7.6	Fast connect security	7
7.7	Encrypted ITU-T H.245 DTMF	10
7.8	Diffie-Hellman operation	11
8	Signalling and procedures	15
8.1	Revision 1 compatibility.....	16
8.2	Version 3 feature indication	16
8.3	Key transport	17
8.4	Enhanced OFB mode.....	18
8.5	Key management	19
8.6	Key update and synchronization	24
8.7	Non-terminal interactions.....	28
8.8	Multipoint procedures	29
9	Media stream encryption procedures.....	29
9.1	Media session keys	30
9.2	Media anti-spamming.....	31
9.3	RTP/RTCP issues	33
9.4	Triple-DES in outer CBC mode	35
9.5	DES algorithm operating in EOFB mode.....	36
9.6	Triple-DES in outer EOFB mode	36
10	Lawful interception.....	36
11	List of object identifiers.....	36

Recommendation ITU-T H.235.6

H.323 security: Encryption profile with native ITU-T H.235/H.245 key management

1 Scope

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

2 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 H.225.0] | Recommendation ITU-T H.225.0 v7 (2009), <i>Call signalling protocols and media stream packetization for packet-based multimedia communication systems.</i> |
| [ITU-T H.235v1] | Recommendation ITU-T H.235 v1 (1998), <i>Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals.</i> |
| [ITU-T H.235v2] | Recommendation ITU-T H.235 v2 (2000), <i>Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals.</i> |
| [ITU-T H.235v3] | Recommendation ITU-T H.235 v3 (2003), <i>Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals</i> plus Corrigendum 1 (2005). |
| [ITU-T H.235.0] | Recommendation ITU-T H.235.0 (2014), <i>H.323 security: Framework for security in ITU-T H-series (ITU-T H.323 and other ITU-T H.245-based) multimedia systems.</i> |
| [ITU-T H.235.1] | Recommendation ITU-T H.235.1 (2005), <i>H.323 security: Baseline security profile.</i> |
| [ITU-T H.235.2] | Recommendation ITU-T H.235.2 (2005), <i>H.323 security: Signature security profile.</i> |
| [ITU-T H.235.3] | Recommendation ITU-T H.235.3 (2005), <i>H.323 security: Hybrid security profile.</i> |
| [ITU-T H.245] | Recommendation ITU-T H.245 (2005), <i>Control protocol for multimedia communication.</i> |
| [ITU-T H.323] | Recommendation ITU-T H.323 (2009), <i>Packet-based multimedia communications systems.</i> |
| [ITU-T H.530] | Recommendation ITU-T H.530 (2002), <i>Symmetric security procedures for H.323 mobility in H.510.</i> |



[ITU-T X.800]	Recommendation ITU-T X.800 (1991) ISO/IEC 7498-2:1989, <i>Security architecture for Open Systems Interconnection for CCITT applications</i> .
[ITU-T X.803]	Recommendation ITU-T X.803 (1994) ISO/IEC 10745:1995, <i>Information technology – Open Systems Interconnection – Upper layers security model</i> .
[ITU-T X.810]	Recommendation ITU-T X.810 (1995) ISO/IEC 10181-1:1996, <i>Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview</i> .
[ITU-T X.811]	Recommendation ITU-T X.811 (1995) ISO/IEC 10181-2:1996, <i>Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework</i> .
[IETF RFC 2198]	IETF RFC 2198 (1997), <i>RTP Payload for Redundant Audio Data</i> .
[IETF RFC 2246]	IETF RFC 2246 (1999), <i>The TLS Protocol Version 1.0</i> .
[IETF RFC 2401]	IETF RFC 2401 (1998), <i>Security Architecture for the Internet Protocol</i> .
[IETF RFC 2833]	IETF RFC 2833 (2000), <i>RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals</i> .
[IETF RFC 3546]	IETF RFC 3546 (2003), <i>Transport Layer Security (TLS) Extensions</i> .
[ISO/IEC 9797-1]	ISO/IEC 9797-1:2011, <i>Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher</i> .
[ISO/IEC 9797-2]	ISO/IEC 9797-2:2011, <i>Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function</i> .
[ISO/IEC 10116]	ISO/IEC 10116:2006, <i>Information technology – Security techniques – Modes of operation for an n-bit block cipher</i> .
[ISO/IEC 10118-3]	ISO/IEC 10118-3:2004, <i>Information Technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions</i> .
[NIST FIPS 197]	NIST FIPS 197 (2001), <i>Advanced Encryption Algorithm (AES)</i> . < http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf >

3 Terms and definitions

For the purposes of this Recommendation, the definitions given in clause 3 of [ITU-T H.323], [ITU-T H.225.0] and [ITU-T H.245] apply. Some of the terms used in this Recommendation are also defined in [ITU T X.800], [ITU-T X.803], [ITU-T X.810] and [ITU-T X.811].

The **session key** for encrypting media streams is generated by the master for each RTP session of a call and exchanged via an OLC. The generated session key is encrypted with a key that is derived from the agreed Diffie-Hellman **shared secret** that both end points have computed. In this case, the DH-shared secret acts as Master Key for protection of the session key(s).

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

3DES	Triple Data Encryption Standard algorithm
AES	Advanced Encryption Standard algorithm
ASN.1	Abstract Syntax Notation One
CBC	Cipher Block Chaining
CFB	Cipher Feedback
DES	Data Encryption Standard
DH	Diffie-Hellman
DTMF	Dual Tone Multi-Frequency
ECB	Electronic Code Book
EOFB	Enhanced Output Feedback mode
EP	End Point
FEC	Forward Error Correction
GK	Gatekeeper
HMAC	Hashed Message Authentication Code
IPsec	Internet Protocol Security
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	Rollover Counter
RSA	Rivest, Shamir and Adleman
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport 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", for examples refer to clauses 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, though 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 Encryption security profile

The 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 set-up procedures; e.g., the Diffie-Hellman key agreement and other key management functions.

ITU-T H.323 entities may implement this Recommendation for achieving 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, ITU-T 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 encryption. In this case, Diffie-Hellman key agreement and other key management procedures are not necessary.

For optional confidentiality, the suggested scheme is encryption using AES, 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 encryption. In this case, Diffie-Hellman key agreement and other key management procedures are also not necessary.

This Recommendation further profiles the list of candidate encryption algorithms that Annex D of [ITU-T H.235v2] or [ITU-T H.235v3] 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 [ITU-T H.235v2] or [ITU-T H.235v3].

ITU-T H.323 entities that implement this Recommendation with version 4 of Recommendation ITU-T H.235 or higher versions shall offer 128-bit AES as the preferred encryption algorithm in their offered security capabilities. Those ITU-T H.323 entities may additionally and optionally also offer 168-bit Triple-DES as an encryption algorithm to achieve higher interoperability with ITU-T

H.323 systems that have implemented the encryption features in Annex D of [ITU-T H.235v2] and [ITU-T H.235v3]. Since 56-bit DES and 56-bit RC2-compatible (exportable) encryption algorithms are no longer considered sufficiently secure, ITU-T H.323 entities should not offer these particular weak encryption algorithms unless there is a specific need, such as achieving interoperability with encryption systems in Annex D of [ITU-T H.235v2] and [ITU-T H.235v3]. ITU-T H.323 entities having higher security requirements may offer 192-bit or 256-bit AES as an optional algorithm.

ITU-T H.323 entities that implement this Recommendation with version 4 of Recommendation ITU-T H.235 should accept AES with the highest key length offered if allowed by their security policy. These ITU-T H.323 entities should additionally accept 168-bit Triple-DES if AES was not offered or is otherwise not allowed by their security policy. These ITU-T H.323 entities 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 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 ITU-T 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 encryption profile. The encryption profile is specified in clauses 7, 8 and 9.

Table 1 – Encryption profile

Security services	Call functions									
	RAS	ITU-T H.225.0	ITU-T H.245	RTP						
Authentication and integrity										
Non-repudiation										
Confidentiality				56-bit DES	56-bit RC2- compa tible	168- bit triple -DES	128- bit AES	192- bit AES	256- bit AES	
				CBC-mode or EOFB-mode						
Access control										
Key management		Authenticated Diffie- Hellman key- exchange	Integrated ITU-T 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 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 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 clause 9.3.1.
- Padding, if needed, is to occur as described in clause 9.3.2.

The payload shall be encrypted using the negotiated encryption algorithm ("X", "Y", "Z", "Z3", "Z4", "Z5") according to the procedures described in clauses 9 and 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 ITU-T 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 ITU-T H.245 channel operation

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

7.2 Unsecured ITU-T H.245 channel operation

Alternatively, the ITU-T 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 ([IETF RFC 2246], [IETF RFC 3546]) or IPsec ([IETF 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 clause 5.2 of [ITU-T H.245] (Capability exchange procedures) and the appropriate ITU-T H-series system Recommendation, end points exchange capabilities using ITU-T H.245 messages. These capability sets may now contain definitions which indicate security

and encryption parameters. For example, an end point might provide capabilities to send and receive ITU-T H.261 video. It may also signal the ability to send and receive encrypted ITU-T 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, end points may supply both independent and dependent encrypted codecs in their exchange. This will allow end points to scale their security capabilities based upon the overheads and resources available.

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

7.4 Master role

The ITU-T 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 end point 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

End points 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 end point (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

End points may deploy the fast connect procedure (see clauses 8.1.7 and 8.1.7.1 of [ITU-T H.323]) using the fast start element for securely exchanging key material (master key and session encryption keys). The procedures given in clause 7.6.1 describe "plain" fast start that does not use multiple offered encryption algorithms whereas clause 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 clause 7.8. During the SETUP-to-CONNECT sequence, a Diffie-Hellman (DH) exchange shall be performed, this seeds both end points with a shared secret. The **ClearToken** field of the **CryptoToken** fields shall contain a **dhkey** for a key length up to 2048 bits or a **dhkeyext** for a key length greater than 2048, 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 Appendix E.2 of [b-IETF RFC 2412].

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

In either direction with an ITU-T 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 end point identifier of the sender and **tokenOID** set to "E". Any intermediate ITU-T 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 ITU-T H.245 Cap exchange, end points present **H235SecurityCapability** entries for the codecs that they support. Each codec is associated with a separate ITU-T H.235 security capability. According to Table 6, these capabilities should indicate support for 128-bit AES-CBC (OID – "Z3"), 192-bit AES-CBC (OID – "Z4"), 256-bit AES-CBC (OID – "Z5"), 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 clause 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, so 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 content 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 clause 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 the 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

