INTERNATIONAL TELECOMMUNICATION UNION

# ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

# H.233

(11/2002)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Systems aspects

## Confidentiality system for audiovisual services

ITU-T Recommendation H.233

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.399 |
| 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 |

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

# ITU-T Recommendation H.233

## Confidentiality system for audiovisual services

### Summary

This Recommendation describes the confidentiality part of a privacy system suitable for use in narrow-band audiovisual services conforming to ITU-T Recs H.320, H.221, H.230 and H.242. Although an encryption algorithm is required for such a privacy system, the specifications of such algorithms are not all included here: the system caters for more than one specific algorithm. Some of those algorithms and their parameters are defined in Annex A. A privacy system consists of two parts, the confidentiality mechanism or encryption process for the data, and a key management subsystem as described in ITU-T Rec. H.234.

This revised version of ITU-T Rec. H.233 introduces a number of corrections and clarifications to the original version and, more importantly, introduces the description on the usage of Triple DES and AES encryption in applicable H.320.x-series Recommendations.

### Source

ITU-T Recommendation H.233 was revised by ITU-T Study Group 16 (2001-2004) and approved under the WTSA Resolution 1 procedure on 29 November 2002.

## 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.

## 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 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.233

## Confidentiality system for audiovisual services

### 1 Scope

A privacy system consists of two parts, the confidentiality mechanism or encryption process for the data, and a key management subsystem.

This Recommendation describes the confidentiality part of a privacy system suitable for use in narrow-band audiovisual services conforming to ITU-T Recs H.221, H.230 and H.242. Although an encryption algorithm is required for such a privacy system, the specification of such an algorithm is not included here: the system caters for more than one specific algorithm.

The confidentiality system is applicable to point-to-point links between terminals or between a terminal and a Multipoint Control Unit (MCU); it may be extended to multipoint working in which there is no decryption at the MCU, but this is for further study.

### 2 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.

[1] ITU Recommendation H.221 (1999), *Frame structure for a 64 to 1920 kbit/s channel in audiovisual teleservices*.

[2] ITU Recommendation H.242 (1999), *System for establishing communication between audiovisual terminals using digital channels up to 2 Mbit/s*.

[3] ITU Recommendation H.230 (1999), *Frame-synchronous control and indication signals for audiovisual systems*.

[4] ITU Recommendation X.680 (2002), *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.

[5] ITU Recommendation H.234 (2002), *Encryption key management and authentication system for audiovisual services*.

[6] ISO 8732:1988, *Banking – Key management (wholesale).*

### 3 Abbreviations

This Recommendation uses the following abbreviations:

| | |
|---|---|
| AIA | Audio Indicate Active (Control & indication codes) (see [3]) |
| AIM | Audio Indicate Muted (Control & indication codes) (see [3]) |
| BAS | Bit-rate Allocation Signal (see [1]) |
| CRC4 | 4-bit Cyclic Redundancy Check (see [1]) |
| ECS | Encryption Control Signal (see [1]) |

| | |
|---|---|
| FAS | Frame Alignment Signal (see [1]) |
| H.221 | H.221 framing/frame structure (see [1]) |
| ILC | Identifier, Length, Content |
| IV | Initialization Vector |
| LSB | Least Significant Bit |
| MCU | Multipoint Control Unit |
| MLP | MLP logical channel (see [1]) |
| MSB | Most Significant Bit |
| OFB | Output feedback |
| SE | Session Exchange |
| SV | Starting Variable |
| TOFB | TDEA Output Feedback |
| VIS | Video Indicate Suppressed (Control and indication codes) (see [3]) |

## 4 Properties of the system specified

### 4.1 Confidentiality

1) Confidentiality is independent of other privacy services provided by the system; keys are provided by other mechanisms such as that described in ITU-T Rec. H.234 on Authentication and Key Management, or may be manually entered.

2) It is applicable to audiovisual signals framed according to ITU-T Rec. H.221, at transfer rates of $p$ × 64 kbit/s where $p$ takes any one value from 1 to 30. In accordance with ITU-T Rec. H.221, the FAS, BAS, and ECS channels of the frame structure are not encrypted.

3) Confidentiality is given to all user audio, video and data transmissions, these signals being encrypted together under the same key (this currently includes MLP data, according to Annex A/H.221, though this aspect is for further study).

4) The system is independent of the encryption algorithm used; some algorithms are currently provided for, and further algorithms could be added.

5) The confidentiality mechanism is capable of working in point-to-point calls, and also in multipoint calls where decryption is permitted at the MCU (the so-called "trusted MCU").

### 4.2 Algorithm specification

The specification of algorithms is not included in this Recommendation, which caters to a wide range of encryption algorithms. The specifications may be defined in Annex A, or shall be available elsewhere (see 5.2) and shall contain the following details:

– lengths of initialization vector and session keys;

– generation of starting variable from initialization vector.

## 5 The confidentiality mechanism

### 5.1 Description of operation

Figure 1 gives a block diagram of a link encryptor. It consists of an encryptor block and a decryptor block. The encryptor takes in user data and enciphers it to form enciphered data. The decryptor takes enciphered data and deciphers it to obtain user data.

Two channels are needed to connect the encryptor and decryptor. One is used to transmit the enciphered user data. The second is an unenciphered channel known as the Encryption Control Signal (ECS) which is used to pass control information from the encryptor to the decryptor. Although these two channels are shown physically separated, in practice, they are multiplexed into a single frame structure as shown in ITU-T Rec. H.221.

Additive-stream encipherment techniques are used (see 5.2).

Keys are provided by other mechanisms and are presented to the confidentiality mechanism as required. They are used by the encryptor and decryptor synchronously with the data, the key-loading synchronization flag being sent via the control channel (see L in 5.1.3).

Data encipherment is controlled from the encryptor: the encryption ON/OFF flag is sent via the control channel to indicate when data is being enciphered. The decryptor responds to this flag and deciphers data when requested.

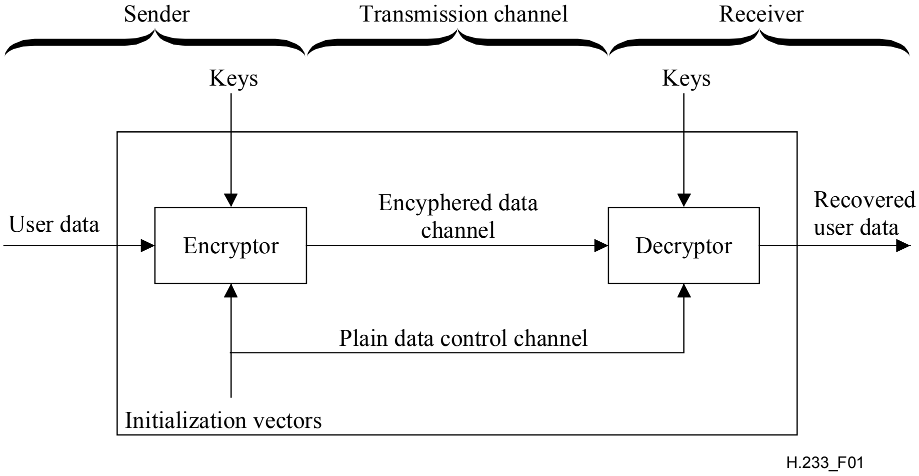


**Figure 1/H.233 – Block diagram of a link encryptor**

### 5.1.1 Controls and indication within the H.221 frame

To indicate the presence of a confidentiality system within a terminal the BAS code "Encryption capability" shall be transmitted. If this capability is signalled from both ends of a link, the Encryption Control Signal (ECS) channel may be opened in each direction by use of the encrypt-on BAS command; the ECS channel may be closed using the command encrypt-off, but this shall be preceded by the transmission of the encryption-off flag within the channel itself (see below). If a terminal receives the BAS command encrypt-off without first receiving the encryption-off flag, the user shall be alerted to a possible intrusion or malfunction of the confidentiality system.

In cases where an H.221-framed signal is in use in one direction only, the ECS channel may be activated without use of the capability mechanism: the mechanism to ensure that the receiving end is able to decrypt the chosen algorithm, etc., is outside the scope of this Recommendation.

### 5.1.2 Message formats

The messages used by the encryption system for key distribution and authentication are formatted in a nested ILC (Identifier, Length, Content) form as described in ITU-T Rec. X.680 [4]. The length may be encoded in short form or long form. The indefinite form as defined in [4] will not be used.

A short description of some of the ITU-T Rec. X.680 [4] definitions used within this Recommendation is given below.

#### 5.1.2.1 Identifier

An identifier is an octet with the structure shown next.

| MSB | | | | | | | LSB |
|---|---|---|---|---|---|---|---|
| c | c | p | t | t | t | t | t |

| | |
|---|---|
| c | Tag class |
| p | Primitive/constructor (0/1) |
| t | Tag |

The tag class defines the type of identifier and takes a value of 10 or 11 (context specific).

The primitive/constructor (P) bit indicates whether the content is primitive or whether it is composed of nested elements.

The 5-bit tag uniquely defines the identifier (according to its class).

Thus, all identifiers in this Recommendation have the octet form: 10 P $t_1$ $t_2$ $t_3$ $t_4$ $t_5$ or 11 P $t_1$ $t_2$ $t_3$ $t_4$ $t_5$.

#### 5.1.2.2 Length

The length specifies the length in octets of the contents and is itself variable in length.

The short form is one octet long and shall be used in preference to the long form when L is less than 128. Bit 8 has the value zero and bits 7-1 encode L as an unsigned binary number whose MSB and LSB are bit 7 and bit 1, respectively.

The Long form is from 2 to 127 octets long and is used when L is greater than, or equal to, 128 and less than 2 to the power 1008. Bit 8 of the first octet has the value one. Bits 7-1 of the first octet encode a number one less than the size of the length in octets as an unsigned binary number whose MSB and LSB are bit 7 and bit 1, respectively. L itself is encoded as an unsigned binary number whose MSB and LSB are bit 8 of the second octet and bit 1 of the last octet, respectively. This binary number shall be encoded in the fewest possible octets, with no leading octets containing the value 0.

#### 5.1.2.3 Bit string

A bit string in primitive form has the bits packed eight to an octet and preceded by an octet that encodes the number of unused bits in the final octet of the contents, from zero to seven, as an unsigned binary number those MSB and LSB are bit 8 and bit 1, respectively.

### 5.1.3 Unenciphered ECS channel

The confidentiality system requires the use of an unenciphered control channel between encryptor and decryptor. Only one control channel per link encryption system is required. The same control channel is used in association with the encryption of the audio, video and any data that may be present.

The content of the ECS channel is structured in blocks of 128 bits, synchronous with the H.221 multiframe (see Figure 2); thus the first bit of the block is bit 8 of octet 17 of frame number 0 in a multiframe. There are two types of block: Session Exchange (SE) and Initialization Vector (IV). The information contained within an IV block takes effect from the start of the next multiframe, and remains effective until another IV has been sent. The ECS channel shall always contain either an IV block or an SE block. It shall be noted that according to some algorithm definitions the same IV may be loaded repeatedly; the choice as to whether or not to do this would be based on the trade-off between faster recovery from errors and additional security.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
|  | Bit No. |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12-119 | 120-127 |
| SE Type | 0 | n | n | s | s | s | s | s | e | e | e | e | message | spare |
|  | Bit No. |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12-107 | 108-127 |
| IV Type | 1 | n | n | A | C | C | L | s | e | e | e | e | IV | spare |

**Figure 2/H.233 – Control channel blocks**

The block contains the following:

1) Header (12 bits), consisting of:
   - Bit 0 to select type:
     - 0 = SE (Session Exchange)
     - 1 = IV (Initialization Vector)
   - Bits 1 and 2 to identify the blocks of a multi-block sequence:
     - 00 for a single block, not followed by related blocks
     - 01 for block #1 of a sequence of several blocks
     - 10 for an intermediate block in a sequence
     - 11 for the last block of a sequence
   - Bits 3-7 of SE-type block: spare (s) set to "0"
   - Bit 3 of IV-type block to indicate encryption on/off (A):
     - 1 = ON, 0 = OFF
   - Bits 4 and 5 of IV-type block to give length of IV (CC):
     - 00 = 64 bits + 32 bits error correction
     - 01, 10, 11 reserved
   - Bit 6 of IV-type block: reserved for key-loading synchronization (L)
   - Bit 7 of IV-type block: spare (s) set to "0"
   - Bits 8-11: error correction (e) for bits 0-7

2) SE Blocks: 108 bits structured as 9 × (8 information bits + 4 error correction bits)

   IV Blocks: System Initialization Vector or part thereof (64 bits), with error protection (32 bits).

3) SE Blocks: 8 spare bits

   IV Blocks: 20 spare bits; provide an interval for the system to act upon the information received, and may also provide for future enhancement.

#### 5.1.3.1 Session exchange blocks

In SE-type blocks, the 116 bits following the 8 + 4 bit header are structured as 9 × (8 + 4) + 8, where the last 8 bits are not used, and the 9 words are each 8 information bits with 4 error-correction bits. At the receiver, the information bits (from more than one block if so indicated in the header) are formed into one stream, consisting of messages on authentication and key management, plus two additional messages P8, P9 defined below for the algorithm capabilities and commands.

All 12 bits of trailing unused words in the SE block shall be set to zero.

#### 5.1.3.1.1 Algorithm capabilities (P8)

| | |
|---|---|
| Message Name: | Here is decryption – algorithms-available information (P8). |
| Message Identifier: | 1 1 P $t_1$ $t_2$ $t_3$ $t_4$ $t_5$ = 1100 0000 |
| Meaning: | Identifies the list of algorithms that a terminal is capable of decrypting |
| Content: | [number 3-255][more bytes] where the first byte gives the number of following bytes. Each set of three bytes indicates an available decryption mechanism using the values listed under media identifiers, algorithm identifiers, and parameter identifiers listed below. |

For example, a terminal capable of decoding DES and FEAL would transmit the P8 message {[11000000][00000110][00000000][00000010][00000000] [00000000][00000001][00000000]}

#### 5.1.3.1.2 Algorithm command (P9)

| | |
|---|---|
| Message Name: | Here is algorithm-in-use information (P9) |
| Message Identifier: | 1 1 P $t_1$ $t_2$ $t_3$ $t_4$ $t_5$ = 1100 0001 |
| Meaning: | When the encryption-ON bit is next set in the IV header, the algorithm used is that specified here in this message. |
| Content: | Encryption scheme bytes (same values as in the capability message P8) |

#### 5.1.3.1.3 Media identifiers

One byte is used for identifying which elements of the audiovisual signal are encrypted. Each bit of this byte corresponds to the following medium:

| | |
|---|---|
| 1st bit (LSB): | Audio 0 = encrypted, 1 = unencrypted |
| 2nd bit: | Video 0 = encrypted, l = unencrypted |
| 3rd bit: | LSD 0 = encrypted, 1 = unencrypted |
| 4th bit: | HSD 0 = encrypted, 1 = unencrypted |
| 5th bit: | reserved for MLP, set to "0" |
| 6th bit: | reserved for H-MLP, set to "0" |
| 7th bit: | reserved for future use, set to "0" |
| 8th bit (MSB): | reserved for future use, set to "0" |

[00000000] represents that the multiplexed signal (except FAS, BAS and ECS) is encrypted. Procedures for other cases are under study.

#### 5.1.3.1.4 Algorithm identifiers

One byte is used for algorithm identification. The definition of the algorithm includes the complete specification as to how the cipher stream is obtained from the current key and IV value. Currently several algorithms have been identified; the following codes shall be used:

| MSB LSB | |
|---|---|
| 0 0 0 0 0 0 0 0 | Not allocated. Reserved for future use |
| 0 0 0 0 0 0 0 1 | FEAL – ISO/IEC 9979 algorithm register No. 0010 |
| 0 0 0 0 0 0 1 0 | DES, Mode 1 – ISO/IEC 9979 algorithm register No. 0004 |
| 0 0 0 0 0 0 1 1 | TDEA – NIST FIPS PUB 46-3 |
| 0 0 0 0 0 1 0 0 | Reserved |

| | |
|---|---|
| 0000 0101 | B-CRYPT – ISO/IEC 9979 algorithm register No. 0001 |
| 0000 0110 | IDEA – ISO/IEC 9979 algorithm register No. 0002 |
| 0000 0111 | Reserved for BARAS (ETSI) |
| 0000 1000 | AES – NIST FIPS PUB 197 |
| Other values | Not allocated. Reserved for future use |

#### 5.1.3.1.5 Parameter identifiers

One byte is used for identifying parameters of the encryption algorithms which are defined in 5.2. Default value is [00000000], which may be used when the algorithm does not need parameter values. For the operational parameters for each encryption method to be used, refer to Annex A.

Equipment shall provide for decryption of at least one of the identified algorithms; if more than one capability is indicated then it may be left to the operator of the system to select the required algorithm for the encryption of the transmitted information.

#### 5.1.3.1.6 Other messages

| | |
|---|---|
| Message Name: | Cannot encrypt (P1) |
| Message Identifier: | 1 0 P $t_1$ $t_2$ $t_3$ $t_4$ $t_5$ = 1000 0001 |
| Meaning: | The sender of this message will not use an encryption system. |
| Content: | This message has no content. |

| | |
|---|---|
| Message Name: | Failure to start encryption system (P2) |
| Message Identifier: | 1 0 P $t_1$ $t_2$ $t_3$ $t_4$ $t_5$ = 1000 0010 |
| Meaning: | The sender of this message has failed to start its encryption system. This could be due to a key exchange failure, but for security reasons, no indication of the cause of failure is given in the message. |
| Content: | This message has no content. |

If it is found necessary to send P1 or P2, or if either of these messages is received, an indication shall be given to the user. The means of indication, and subsequent action, are left to the implementer.

| | |
|---|---|
| Message Name: | Channel idle message (SE_NULL) |
| Message Identifier: | 1 1 P $t_1$ $t_2$ $t_3$ $t_4$ $t_5$ = 1101 1111 |
| Meaning: | The sender of this message is doing some channel filling since it has no other message to send. |
| Content: | This message has no content. |

SE_NULL shall be transmitted when the sender has no capability, command or IV message to transmit. This might happen during an exchange of complementary information that cannot be transmitted simultaneously. For example, exchanges of different size capability sets, or an exchange of keys through the Diffie-Hellman algorithm.

### 5.1.3.2 Initialization vectors

The default length of the IV is 64 bits. The length including error correction is 96 bits. Greater IV lengths can be transmitted using more than one block. The most-significant bit is transmitted first, that is, bit 12 of (first) IV-type block.

### 5.1.3.3 Error protection of control channel information

The information transmitted via the control channel shall be error protected. A [12,8] Hamming code is used for this. The generator and parity check matrices are given in Figure 3.

The same scheme is used for headers, for session exchange messages and for initialization vectors. In each case an 8-bit byte is followed by four error correction bits.

The IV is split into 8 bytes, each byte then having 4 parity bits attached making a total IV plus parity length of 96 bits, in the default case.

| Generator matrix | Parity check matrix |
|---|---|
| 100000001110<br>010000000111<br>001000001010<br>000100000101<br>000010001011<br>000001001100<br>000000100110<br>000000010011 | 1110<br>0111<br>1010<br>0101<br>1011<br>1100<br>0110<br>0011<br>1000<br>0100<br>0010<br>0001 |

H.233_F03

**Figure 3/H.233 – Error correction matrices**

## 5.2 Transmission encryption method

This clause deals with the encryption of the audio, video and any associated data. Encryption will only take place if H.221 multiframe alignment is established.

The encryption system performs the same functions regardless of the transfer rate. Any or all of the user information streams may be encrypted. The encryption system does not need information as to the allocation of the capacity between these various forms of user information, as it encrypts data after multiplexing and decrypts data before demultiplexing. The two directions of transmission are independent: either or both may be encrypted, and different algorithms may be used.

The temporal order of encryption follows that of transmission in a serial stream bit by bit. Data shall be encrypted before any CRC4 calculation takes place. CRC4 calculations are then performed on encrypted data, ensuring that any associated networks are presented with a valid CRC4 code.

A cipher stream is created at both terminals from the current values of the key and the initialization vector; at the encryptor this stream is combined with the bits to be encrypted by modulo-2 addition and, at the decryptor, the encrypted bits are modulo-2-added to the same cipher stream to recover the clear user information.

Initialization vectors (IVs) are created in a random way at the encryptor and are sent to the decryptor via the ECS. They are used synchronously with the data to be encrypted or decrypted. They provide a method of resynchronizing the encryptor and decryptor periodically.

NOTE – Attention shall be paid to the order of IV bits loaded to the encryptor and decryptor, according to the chosen algorithm.

If synchronization is lost, data will be corrupted until a new IV is received. The period for IV transmission is determined by the amount of data loss which can be tolerated until resynchronization is obtained.

Each bit within the channel is treated by the encryption system in one of the following three ways (see Appendix I):

a) a cipher stream is generated and applied: user information (audio, video, data);

b) a cipher stream is generated, but not applied: FAS and BAS in initial and additional channels (see ITU-T Rec. H.221) and ECS; the cipher stream is not stored or delayed for subsequent use, but is lost, and is not used to encrypt any following information;

c) no cipher stream is generated: if the terminal output to line includes channels not forming part of the transfer rate specified in the relevant BAS command (e.g. TS0 and/or TS16 of a primary rate connection, or other channels not transmitted end to end), no cipher stream is generated for these bits.

For the 56 kbit/s transmission as described in Annex B/H.221, a cipher stream is generated for the eighth subchannel but only the first 7 bits are used for modulo-2 addition to the septet signal.

For the restricted 128 kbit/s or higher bit rate transmission, the cipher stream is generated, but not applied, to the stuffed eighth bit in every timeslot.

### 5.3 Procedure for use of the system

When a terminal wishes to start encryption, having received the capability "encryp." (see ITU-T Rec. H.221) in the capset of the remote terminal, it opens the ECS channel and transmits message(s) P8. While waiting to receive a message P8, the terminal fills the ECS channel with a SE_NULL message. On the reception of message(s) P8 from the remote end, it checks whether there are any compatible algorithms/modes: if not, it sends the message P1; if compatible, it sends a message P9 to identify the algorithm/mode which will be used, agrees on the common keys to be used by the encryption algorithm, and then begins the transmission of IV blocks. The key management procedure is done in accordance with ITU-T Rec. H.234. Examples of complete procedures for an encryption session are presented in Appendix II.

P2 may be used in failure recovery procedures (for further study).

## 6 Encryption of MLP channel

For further study.

# Annex A

# Encryption algorithms and their parameters

### A.1 Scope

This annex defines the encryption algorithms for which algorithm identifiers were allocated in 5.1.3.1.4. The definition of the algorithms and their parameters includes the specification as to how the cipher stream is obtained from the current key and IV value.

### A.2 Normative References

[A1] ISO/IEC 9979 Registration No. 0010 (FEAL).

[A2] ISO/IEC 9979 Registration No. 0004 (Data Encryption Standard).

[A3] ISO/IEC 9979 Registration No. 0002 (IDEA).

[A4] NIST Federal Information Processing Standard (FIPS) Publication 46-3 (Triple Data Encryption Algorithm)

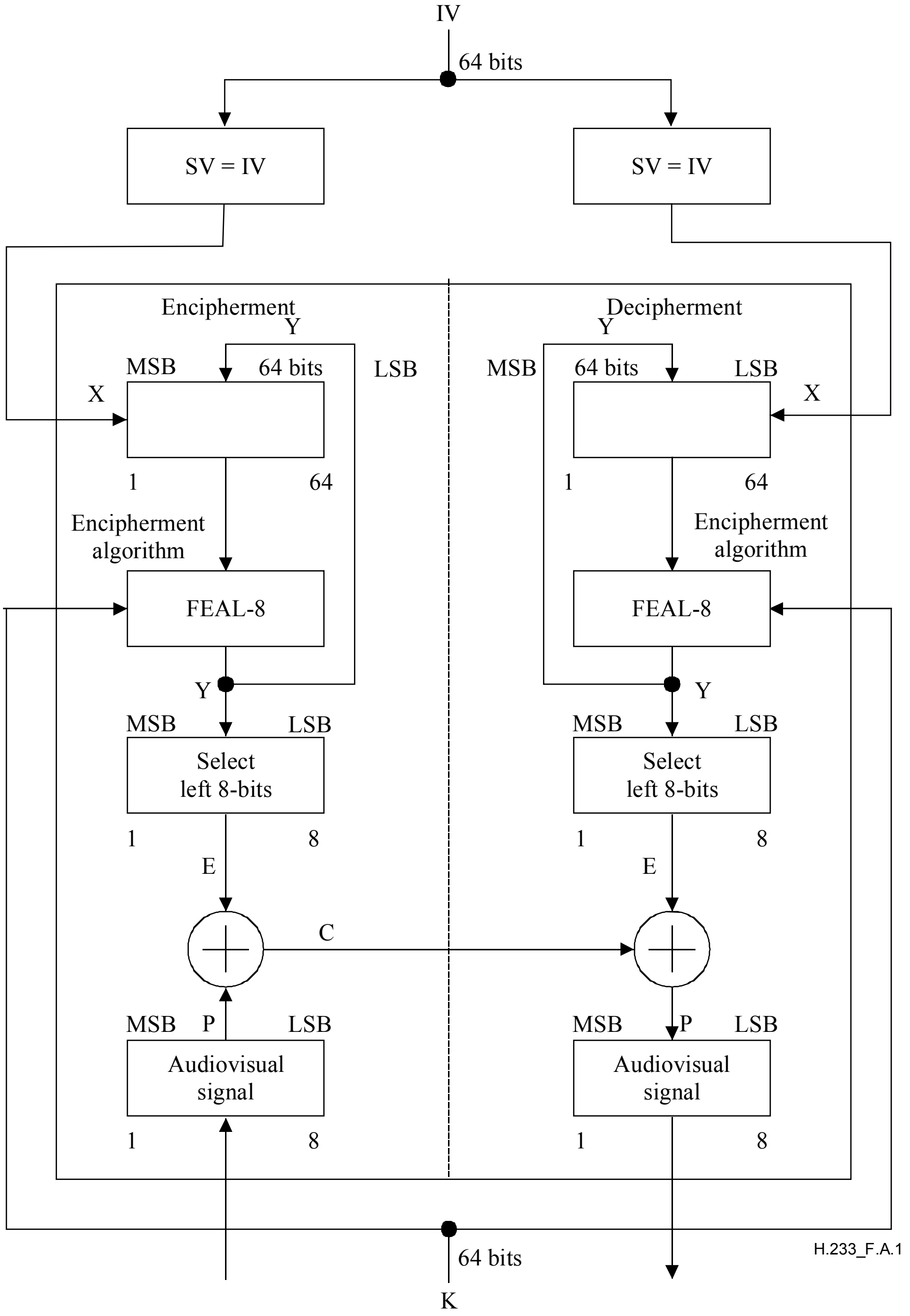
[A5] NIST Federal Information Processing Standard (FIPS) Publication 197 (Advanced Encryption Standard).

### A.3 FEAL

A cipher stream is created at both terminals from the current values of the key and the initialization vector using FEAL-8 (8 round FEAL with 64-bit key) in the OFB mode defined ISO 8372. Details of FEAL algorithm are given in Reference [A1]. At the encryptor this stream is combined with the bits to be encrypted by modulo-2 addition, and at the decriptor the encrypted bits are modulo-2 added to the same cipher stream to recover the clear user information. See Figure A.1.

The Starting Variable (SV) is identical to Initialization Vector (IV). IV is loaded at the start of every multiframe.

Out of the 64 bits output from the encipherment algorithm, the first 8 bits of the MSB side are used for bit-by-bit modulo-2 addition to the 8 bits of the audiovisual signal block; the first bit of the cipher block is modulo-2 added to the first bit of the signal block and the resultant bit is transmitted first through the channel, the second bit of the cipher block is modulo-2 added to the second bit of the signal block and the resultant bit is transmitted next through the channel, and so on. If all of the 8 bits are transmitted, the next cycle of the cipher stream is generated and used for encryption.



| | |
|---|---|
| C | Cypher stream |
| E | Encryption |
| IV | Initialization Vector |
| K | Key |
| P | Plain text |
| SV | Starting Vector |

**Figure A.1/H.233 – Output Feedback (OFB) mode operation for FEAL**

## A.4 DES

The DES algorithm and the methods of applying the cipher stream to the data stream are described in Reference [A2].

DES Mode 1 uses one of the two methods designated OFB-8 and OFB-64. The Starting Variable (SV) is identical to the Initialization Vector (IV). The parameter identifier is set as follows:

| Field value | OFB mode | Number of bits |
|---|---|---|
| MSB LSB | | |
| 0000 0000 | OFB-8 | 8 |
| 0000 0001 | OFB-64 | 64 |

All other values of the parameter identifier are reserved for further study.

## A.5 IDEA

The block cipher algorithm IDEA operates with 64-bit input and output blocks and is controlled by a 128-bit key. It is defined in Reference [A3].

The mode of operation to produce the cipher stream is Output Feedback OFB-8 according to ISO 8372. The Starting Variable is identical to the Initialization Vector (IV).

The method of applying the cipher stream to the data stream is essentially that for OFB defined in ISO 8372. The eight cipher stream bits used for the enciphering of eight data stream bits are the leftmost bits of the 64-bit output block depicted in Figure 1 of Reference [A3].

The Parameter Identifier (see 5.1.3.1.5) is set to [0000 0000] in this mode. Other modes of operation, such as the Cipher Block Chaining mode or the Cipher Feedback mode described in ISO 8372, are for further study.

## A.6 TDEA

The TDEA (or triple DES) algorithm and the methods of applying the cipher stream to the data stream are described in Reference [A4].

The input and output for the TDEA each consist of sequences of 64 bits. These sequences will sometimes be referred to as blocks, and the number of bits they contain will be referred to as their length. The cipher key of the TDEA consists in 112 or 168 bits which is a bundle of two or three different 56 bits DES keys.

The mode of operation to produce the cipher stream is Output Feedback TOFB-64. The Starting Variable (SV) is identical to the Initialization Vector (IV). The parameter identifier is set as follows:

| MSB field value | Key size in bits |
|---|---|
| 00 | 112 |
| 01 | 168 |

| LSB field value | Mode of operation | Number of bits |
|---|---|---|
| 000000 | Reserved | |
| 000001 | TOFB-64 | 64 |

The six LSB bits represent the methods of applying the cipher stream.

The two MSB bits represent the size of the cipher key used to initiate TDEA.

All other values of the parameter identifier are reserved for further study.

Example: TDEA-168 with 64-bits TOFB shall be 0100 0001.

## A.7 AES

The methods of applying the cipher stream to the data stream with AES are defined in Reference [A5].

The input and output for the AES algorithm each consist of sequences of 128 bits. These sequences will sometimes be referred to as blocks, and the number of bits they contain will be referred to as their length. The Cipher Key for the AES algorithm is a sequence of 128, 192 or 256 bits and may be referred to as "AES-128", "AES-192", and "AES-256" respectively.

The Starting Variable (SV) is identical to the length of the Initialization Vector (IV) which shall have a length of 128 bits. The parameter identifier is set as follows:

| **MSB field value** | **Key size in bits** |
|---|---|
| 00 | 128 |
| 01 | 192 |
| 10 | 256 |

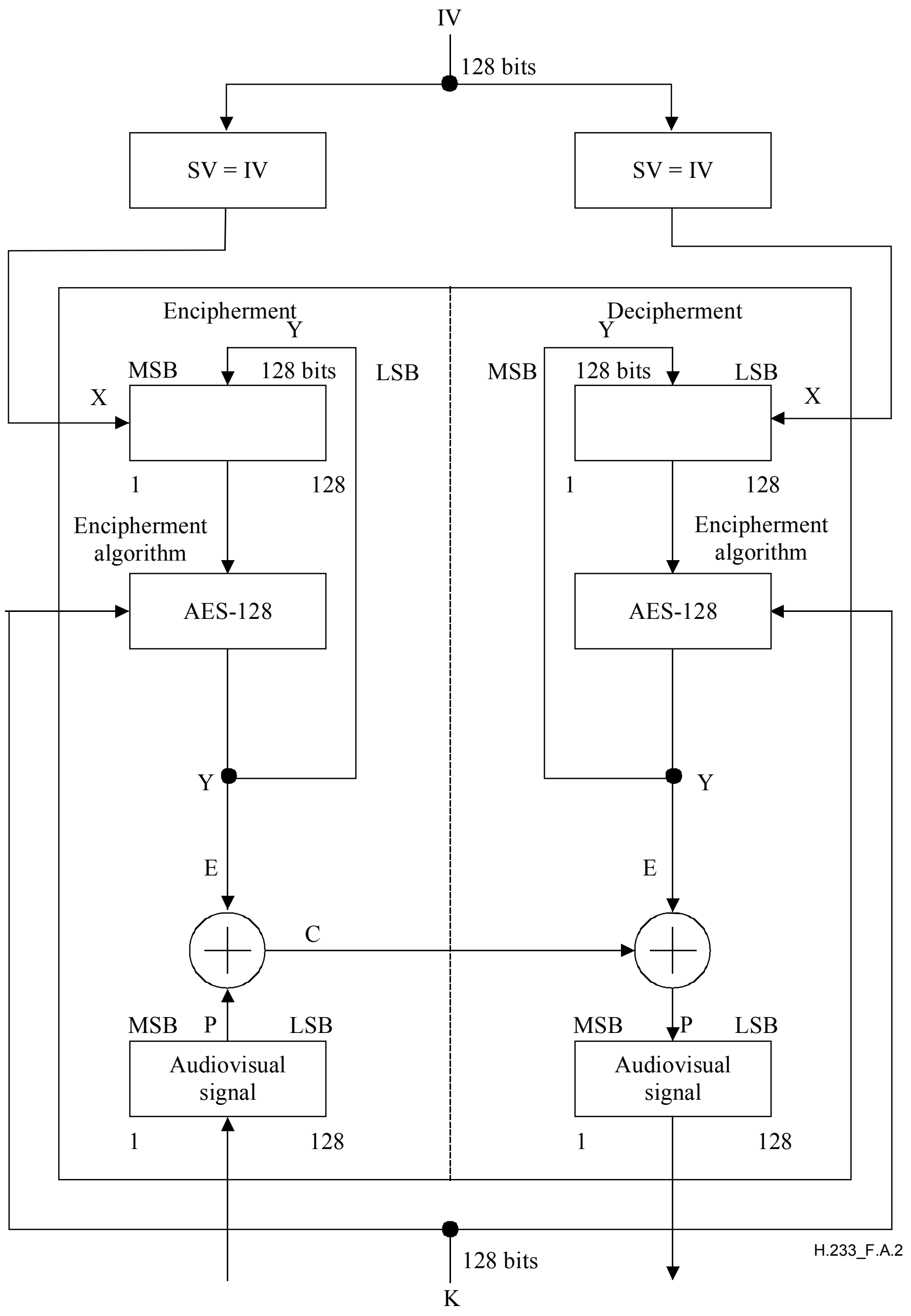
| **LSB field value** | **Mode of operation** | **Number of bits** |
|---|---|---|
| 000000 | Reserved | 128 |
| 000001 | OFB-128 | |

The six LSB bits represent the methods of applying the cipher stream.

The two MSB bits represent the size of the cipher key used to initiate AES.

All other values of the parameter identifier are reserved for further study.

Example: AES-128 with 128-bits OFB shall be 0000 0001.



| | |
|---|---|
| C | Cypher stream |
| E | Encryption |
| IV | Initialization Vector |
| K | Key |
| P | Plain text |
| SV | Starting Vector |

**Figure A.2/H.233 – Output Feedback (OFB) mode operation for AES-128**

# Appendix I

## Encryption and decryption for 2 × B channels

This appendix serves as an illustration for how H.233 encryption/decryption works.

– Cipher stream is generated for all bits;

– Cipher stream is added to all bits except the shaded part.

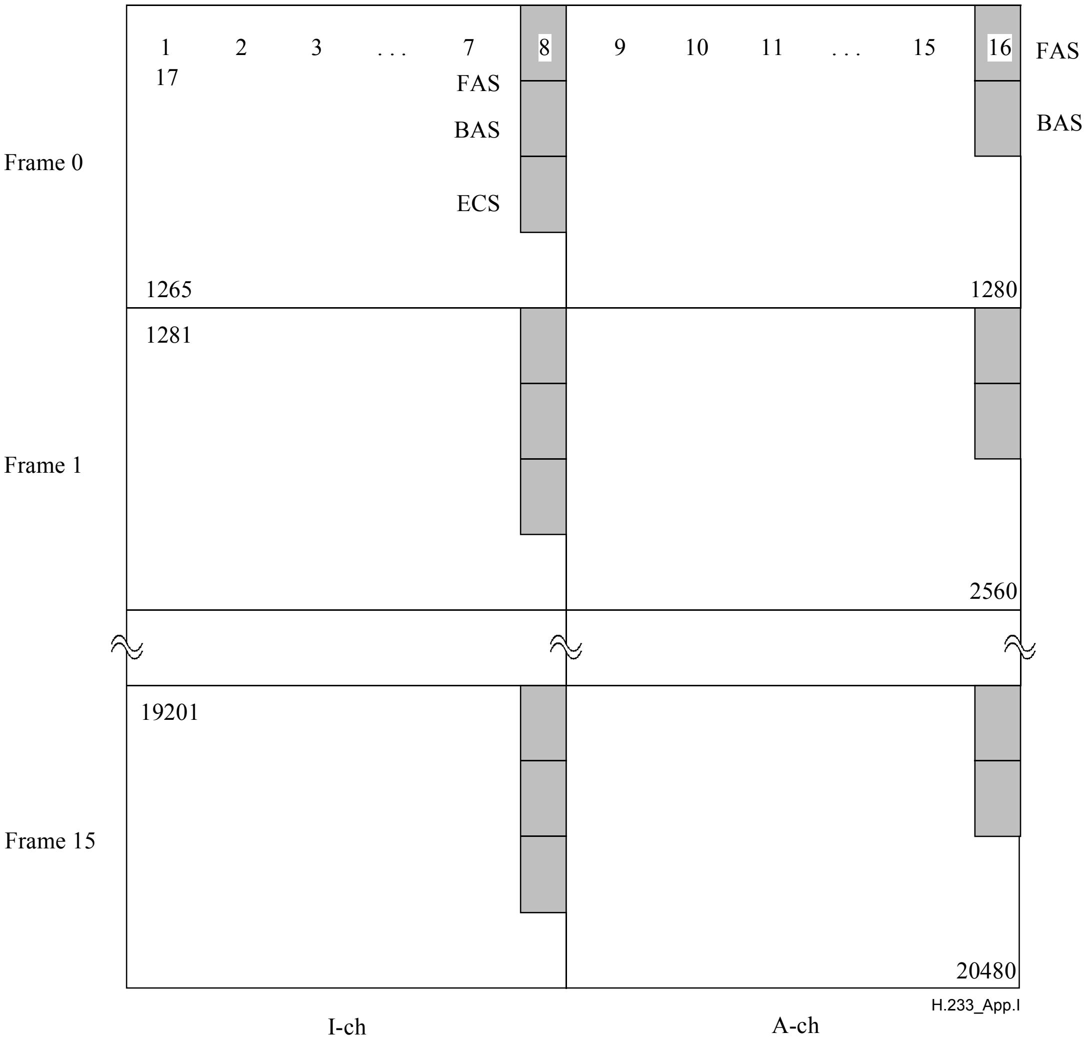
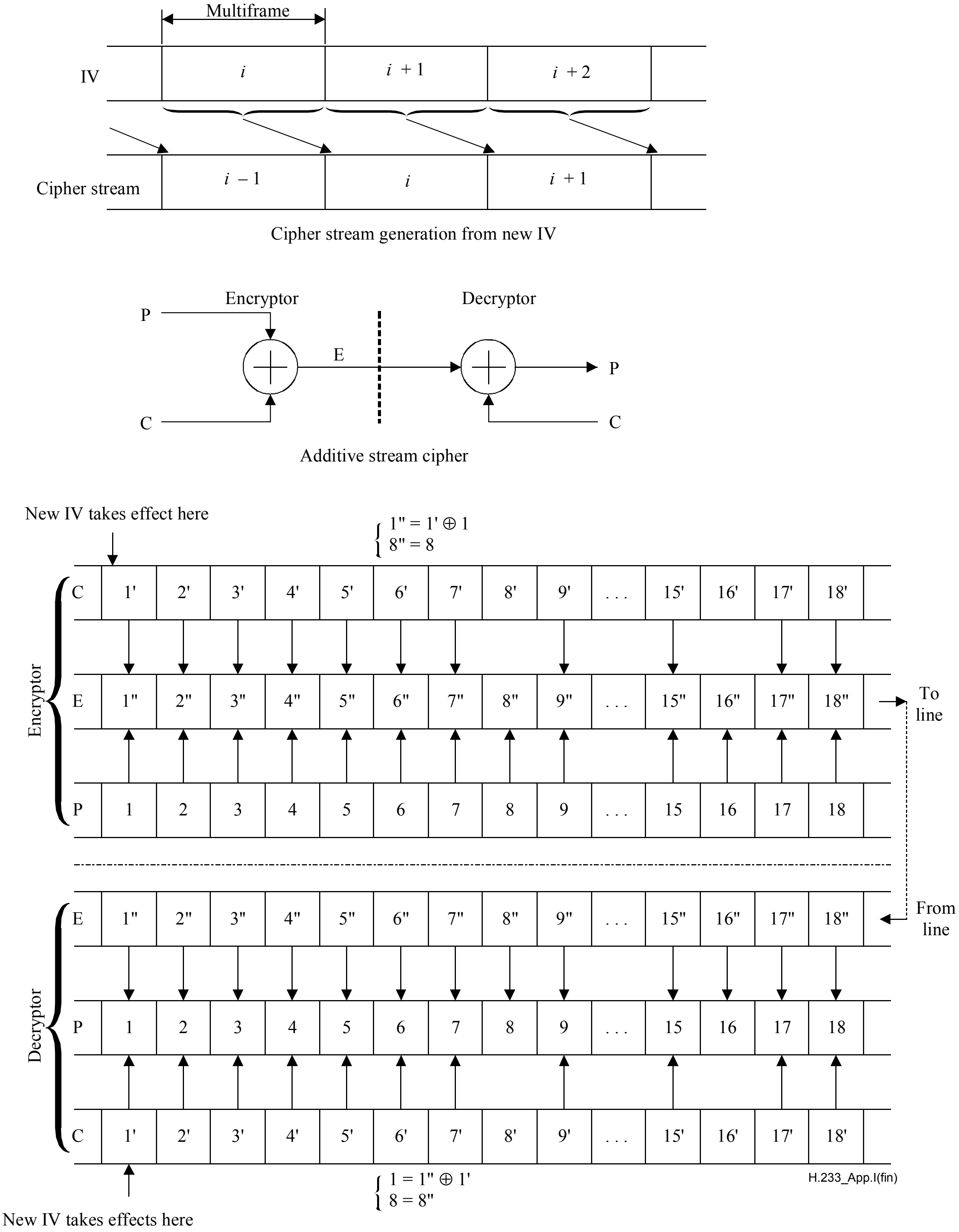


**Figure I.1/H.233 – Bit numbering and unenciphered bits in a multiframe for 2 × B channel**



C Cipher stream
E Encrypted text
P Plain text

**Figure I.2/H.233 – Encryption and decryption process**

# Appendix II

## Audiovisual privacy communication procedure

When privacy is required in an audiovisual communication session, it is achieved by applying H.233, H.234 and other H-series Recommendations. Since necessary elements of communication procedures are defined in several Recommendations, this appendix provides examples for a set of procedures with reference to those Recommendations.

There may be two scenarios for starting privacy in an audiovisual communication:

1) the call is established and in progress when the participants decide to activate encryption;

2) the decision to activate encryption is communicated before the call is set up by external means so that no audiovisual communication happens until the confidentiality mechanism is fully operational.

Tables II.1 and II.2, with focus on privacy aspects, correspond to the two cases, respectively. Procedures are listed in time order where the Extended Diffie-Hellman scheme is used for key distribution.

When privacy communication is invoked, particular attention should be paid to the timing when the audiovisual signals are actually encrypted. Though no particular method is standardized, the terminal design should incorporate appropriate provisions to cope with a few seconds or more which are required before secure communication can be started.

One way may be to allow unencrypted communication until the encrypted signals become available (Scenario 1 above), or another way may be to totally mute audiovisual signals until then (Scenario 2 above). In either case, status of encryption shall be explicitly indicated to users by a lamp sign or other means.

**Table II.1/H.233 – Case of privacy being invoked after the call set-up**

| Time order | Procedure | Message | Channel used | Reference and Notes |
|---|---|---|---|---|
| 1 | Call set-up | BC/LLC/HLC | D-channel | ITU-T Rec. Q.939 |
| 2 | Audio clear path; send AIM if muted; indicate to user if incoming audio muted; indicate outgoing audio unencrypted if not muted. | AIM | BAS | ITU-T Rec. H.230 |
| 3 | Decision to use the privacy between the two parties | | External means | (Note 5) |
| 4 | ECS Capability exchange (Note 1) | Encrypt.(cap) | BAS | ITU-T Rec. H.242 |
| 5 | Opening of ECS channel (Note 1) | Encrypt-on | BAS | ITU-T Rec. H.242 |
| 6 | Identification of available encryption algorithms | P8 | ITU-T Rec. H.233 | |
| 7 | Identification of common key management systems | P0 | ECS(SE) | ITU-T Rec. H.234 |
| 8 | Key management method is known, choose encryption algorithm. | – | (Local) | |

**Table II.1/H.233 – Case of privacy being invoked after the call set-up**

| Time order | Procedure | Message | Channel used | Reference and Notes |
|---|---|---|---|---|
| 9 | Send the chosen algorithm for both session key exchange and audiovisual communications | P9 | | ITU-T Rec. H.233 (Note 2) |
| 10 | Exchange of prime, primitive root and intermediate result | P3, P4 | ECS(SE) | ITU-T Rec. H.234 |
| 11 | Calculation of *key*; rl, r2 and R12. | – | (Local) | ITU-T Rec. H.234 |
| 12 | Presentation of 64 bit check code as 16 hexadecimal digits | (Local) | (Local) | ITU-T Rec. H.234 |
| 13 | Verbal presentation (point-to-point) or check code information from MCU (multipoint) of 64 bit check code – if audio is muted the verbal check can be postponed until after encryption is switched on. | 16 hex digits | Main (p-t-p) or ECS (multipoint) | ITU-T Rec. H.234 |
| 14 | Transmission of initialization vector and 4N bits encrypted random number | P6 | ECS(SE) | ITU-T Rec. H.234 (Note 3) |
| 15 | Encryption on, and initialization vector. | A and IV in ECS | ECS(IV) | ITU-T Rec. H.233 |
| 16 | Indicate outgoing encrypted; unmute, if not automatic; verbal check if required and not already done. | AIA 16 hex digits | (Local)<br>BAS_Main channel | ITU-T Rec. H.230,<br>ITU-T Rec. H.234 |
| 17 | Encrypted audiovisual communications | Audio, video, etc. | Main channel | |
| 18 | Mute audio, suppress video. | AIM, VIS | BAS | ITU-T Rec. H.230 |
| 19 | Encryption off | A in ECS | ECS(IV) | ITU-T Rec. H.233 |
| 20 | Closing of ECS channel (Note 4) | Encrypt-off | BAS | ITU-T Rec. H.242 |
| 21 | Call clear down | – | D-channel | ITU-T Rec. Q.939 |

NOTE 1 – As part of the mode initialization and common mode establishment phase procedures defined in ITU-T Rec. H.242.

NOTE 2 – The encryption algorithm and mode described in Annex A are commonly used for both session key exchange and audiovisual communications.

NOTE 3 – The 4N bits random number is encrypted by the encryption algorithm determined in Procedure 8 with *key* determined in Procedure 10 and initialization vector obtained in this Procedure.

NOTE 4 – As part of the communication termination phase procedures defined in ITU-T Rec. H.242.

NOTE 5 – Outside the scope of standardization.

**Table II.2/H.233 – Case of privacy being decided before the call set-up**

| Time order | Procedure | Message | Channel used | Reference and Notes |
|---|---|---|---|---|
| 0 | Decision to use the privacy between the two parties | | External means | (Note 1) |
| 1 | Call set-up | BC/LLC/HLC | D-channel | ITU-T Rec. Q.939 |
| 2 | Mute audio, suppress video; indicate to user if incoming audio muted or video suppressed | AIM, VIS | BAS | ITU-T Rec. H.230 |
| 3 | ECS Capability exchange (Note 2) | Encrypt.(cap) | BAS | ITU-T Rec. H.242 |
| 4 | Opening of ECS channel (Note 2) | Encrypt-on | BAS | ITU-T Rec. H.242 |
| 5 | Identification of available encryption algorithms | P8 | ECS(SE) | ITU-T Rec. H.233 |
| 6 | Identification of common key management systems | P0 | ECS(SE) | ITU-T Rec. H.234 |
| 7 | Key management method is known, choose encryption algorithm. | – | (Local) | |
| 8 | Send the chosen algorithm for both of session key exchange and audiovisual communications | P9 | | ITU-T Rec. H.233<br>(Note 3) |
| 9 | Exchange of prime, primitive root and intermediate result. | P3, P4 | ECS(SE) | ITU-T Rec. H.234 |
| 10 | Calculation of *key*, rel, r2 and R12. | – | (Local) | ITU-T Rec. H.234 |
| 11 | Presentation of 64 bit check code as 16 hexadecimal digits | (Local) | (Local) | ITU-T Rec. H.234 |
| 12 | (If multipoint) 64 bit check code information from MCU | 16 hex digits | ECS | ITU-T Rec. H.234 |
| 13 | Transmission of initialization vector and 4N bits encrypted random number | P6 | ECS(SE) | ITU-T Rec. H.234<br>(Note 4) |
| 14 | Encryption on, and initialization vector | A and IV in ECS | ECS(IV) | ITU-T Rec. H.233 |
| 15 | Indicate outgoing encrypted; unmute audio, unsuppress video; (if point-to-point) verbal presentation of 64 bit check code. | AIA, VIA<br>16 hex digits | (Local) BAS<br>Main channel | ITU-T Rec. H.230 |
| 16 | Encrypted audiovisual communication | Audio, video, etc. | Main channel | |
| 17 | Mute audio, suppress video. | AIM, VIS | BAS | ITU-T Rec. H.230 |
| 18 | Encryption off | A in ECS | ECS(IV) | ITU-T Rec. H.233 |

**Table II.2/H.233 – Case of privacy being decided before the call set-up**

| Time order | Procedure | Message | Channel used | Reference and Notes |
|---|---|---|---|---|
| 19 | Closing of ECS channel (Note 5) | Encrypt-off | BAS | ITU-T Rec. H.242 |
| 20 | Call clear down | – | D-channel | ITU-T Rec. Q.939 |

NOTE 1 – Outside the scope of standardization.

NOTE 2 – As part of the mode initialization and common mode establishment phase procedures defined in ITU-T Rec. H.242.

NOTE 3 – The encryption algorithm and mode described in Annex A are commonly used for both session key exchange and audiovisual communications.

NOTE 4 – The 4N bits random number is encrypted by the encryption algorithm determined in Procedure 8 with *key* determined in Procedure 10 and initialization vector obtained in this Procedure.

NOTE 5 – As part of the communication termination phase procedures defined in ITU-T Rec. H.242.

## SERIES OF ITU-T RECOMMENDATIONS

| | |
|---|---|
| Series A | Organization of the work of ITU-T |
| Series B | Means of expression: definitions, symbols, classification |
| Series C | General telecommunication statistics |
| 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 | TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits |
| 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 and open system communications |
| Series Y | Global information infrastructure and Internet protocol aspects |
| Series Z | Languages and general software aspects for telecommunication systems |

Printed in Switzerland
Geneva, 2003