EUROPEAN TELECOMMUNICATION STANDARD

FINAL DRAFT

pr **ETS 300 840**

August 1997

Source: ETSI TC-Security

Reference: DE/SEC-002307

ICS: 33.020

Key words: ISDN, multimedia, security

Telecommunications Security; Integrated Services Digital Network (ISDN); Confidentiality system for audiovisual services

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

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

Contents

Blank page

Foreword

This final draft European Telecommunication Standard (ETS) has been produced by the Security (SEC) Technical Committee of the European Telecommunications Standards Institute (ETSI), and is now submitted for the Voting phase of the ETSI standards approval procedure.

The system should support lawful interception of a user's communications in accordance with appropriate national law. Users of this ETS should seek advice from their national authorities.

Proposed transposition dates	
Date of latest announcement of this ETS (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

Blank page

1 Scope

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

This European Telecommunication Standard (ETS) is based on ITU-T Recommendation H.233 [1] and describes the confidentiality part of a privacy system suitable for use in narrowband audio-visual services conforming to ITU-T Recommendations H.221 [2], H.230 [3], H.234 [4], and H.242 [5]. Although an encryption algorithm is required for such a privacy system, the specification of such an algorithm is not included in this ETS. 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 outside the scope of this ETS.

2 Normative references

This ETS incorporates by dated and undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this ETS only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] ITU-T Recommendation H.233: "Confidentiality system for audiovisual services".

[2] ITU-T Recommendation H.221: "Frame structure for a 64 to 1920 kbit/s channel in audiovisual teleservices".

[3] ITU-T Recommendation H.230: "Frame-synchronous control and indication signals for audiovisual systems".

[4] ITU-T Recommendation H.234: "Encryption key management and authentication system for audiovisual services".

NOTE: ITU-T Recommendation H.234 forms the basis of ETS 300 841 [11].

[5] ITU-T Recommendation H.242: "System for establishing communication between audiovisual terminals using digital channels up to 2 Mbit/s".

[6] ITU-T Recommendation X.208: "Specification of Abstract Syntax Notation One (ASN.1) Blue Book Fascicle VIII.4".

[7] ISO/IEC 9979 Registration No. 0001 (B-CRYPT).

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

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

[10] ISO/IEC 9979 Registration No. 0011 (BARAS).

[11] ETS 300 841: "Telecommunications Security; Integrated Services Digital Network (ISDN); Encryption key management and authentication system for audiovisual services".

[12] ITU-T Recommendation Q.939: "Typical DSS 1 service indicator codings for ISDN telecommunications services".

[13] ISO/IEC 8372: "Information processing -- Modes of operation for a 64-bit block cipher algorithm".

3 Abbreviations

For the purposes of this ETS, the following abbreviations apply:

AIM, AIA, VIS	control & indication codes (see ITU-T Recommendation H.230 [3])
ASN.1	Abstract Syntax Notation nº 1
BARAS	Baseline Algorithm Recommended for use in Audiovisual Systems
BAS	Bit Allocation Signal (see ITU-T Recommendation H.221 [2])
CRC4	Cyclic Redundancy Check 4 (see ITU-T Recommendation H.221 [2])
DES	Data Encryption Standard
ECS	Encryption Control Signal (see ITU-T Recommendation H.221 [2])
FAS	Frame Alignment Signal (see ITU-T Recommendation H.221 [2])
FEAL	Fast Encryption Algorithm
H.221	"H.221 framing/frame structure" (see ITU-T Recommendation H.221 [2])
IDEA	International Data Encryption Algorithm
ILC	Identifier, Length, Content
ISDN	Integrated Services Digital Network
IV	Initialization Vector
L	Length parameter
LSB	Least Significant Bit
MCU	Multipoint Control Unit
MLP	"MLP" logical channel (see ITU-T Recommendation H.221 [2])
MSB	Most Significant Bit
OFB	Output Feedback
SE	Session Exchange
SV	Starting Variable

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 Recommendation H.234 [4], or may be manually entered.

2) It is applicable to audio-visual signals framed according to ITU-T Recommendation H.221 [2], at transfer rates of p × 64 kbit/s where p takes any one value from 1 to 30. In accordance with ITU-T Recommendation H.221 [2], the frame structure itself is not encrypted.

3) Confidentiality is given to all user audio, video and data transmissions, these signals being encrypted together under the same key.

   NOTE: This currently includes MLP data, according to ITU-T Recommendation H.221 [2], annex A, 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 ETS, which caters to a wide range of encryption algorithms. The specifications shall be available elsewhere (see subclause 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 in ITU-T Recommendation H.233 [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.

Connecting the encryptor and decryptor are two channels. 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 data stream.

Additive-stream encipherment techniques are used (see subclause 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, a load new key flag being sent via the control channel (see **L** in subclause 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.

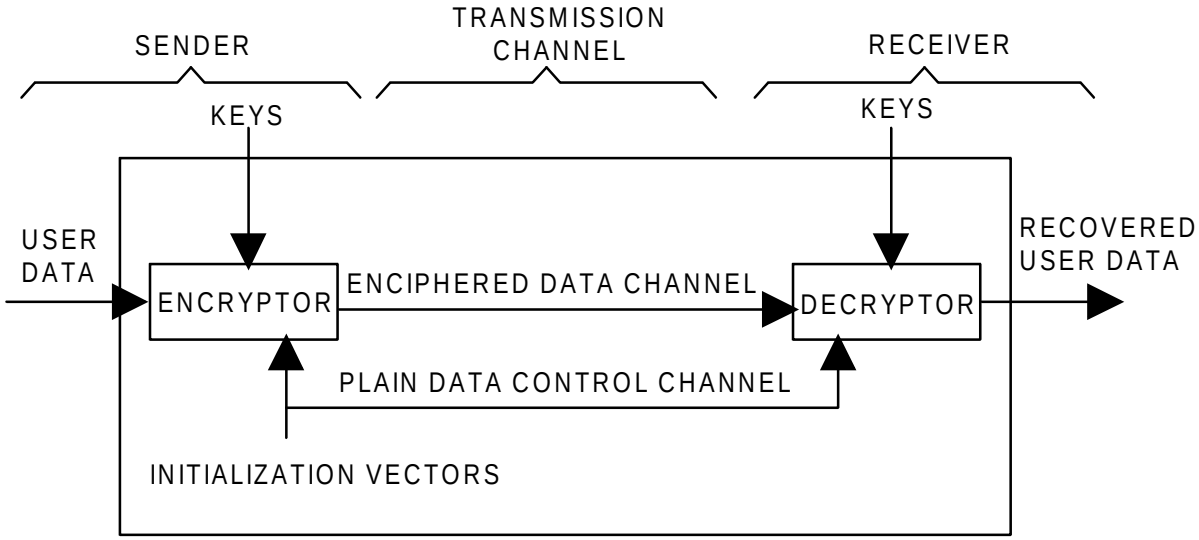


Figure 1: Block diagram of the link encryption system

5.1.1 Controls and indication within the H.221 frame

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

In cases where a ITU-T Recommendation H.221 [2]-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 then outside the scope of this ETS.

5.1.2 Message formats

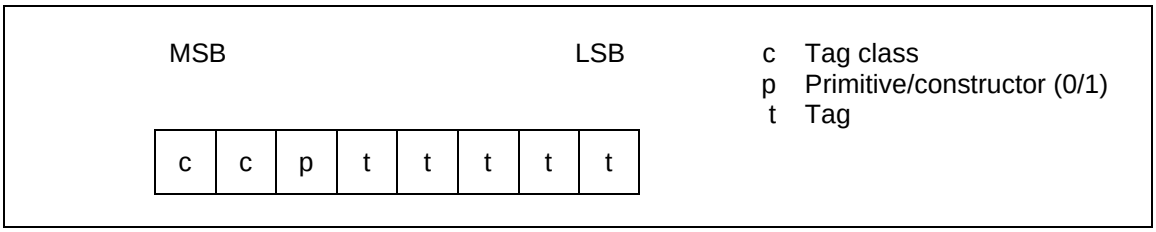
The messages used by the encryption system for key distribution and authentication are formatted in a nested Identifier, Length, Content (ILC) form as described in ITU-T Recommendation X.208 [6]. The length may be encoded in short form or long form. The indefinite form as defined in ITU-T Recommendation X.208 [6] will not be used.

The messages described in this recommendation allow the various messages to be identified by the encryption system. The messages used by the encryption system shall also be identified by the message system as belonging to the encryption system. The descriptions of the identifiers used by the messaging system for that purpose are beyond the scope of this recommendation.

A short description of some of the definitions in ITU-T Recommendation X.208 [6] used within this proposal is given in subclauses 5.1.2.1 to 5.1.2.3.

5.1.2.1 Identifier

An identifier is an octet with the structure shown next.



The Tag Class defines the type of identifier which will be 10 or 11 (context specific) for the identifiers defined within this ETS.

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 ETS have the octet form: 1 0 P t_1 t_2 t_3 t_4 t_5 or 1 1 P t_1 t_2 t_3 t_4 t_5.

5.1.2.2 Length (L)

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 Most Significant Bit (MSB) and Least Significant Bit (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 1 008. 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 whose 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 in ITU-T Recommendation H.233/2 [1]); 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 a SE block.

NOTE: 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.

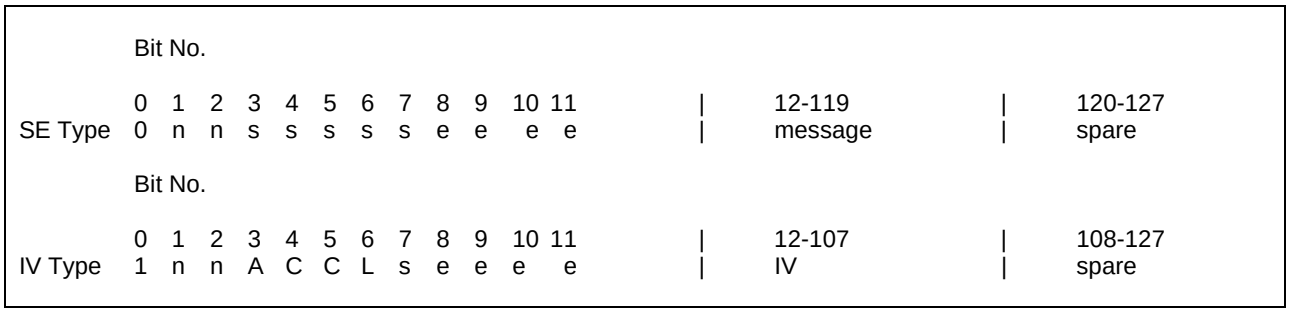


Figure 2: Control channel blocks

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;

- 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**);

- all other bits: spare (s) set to "0";

- bits 8-11: error correction 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.

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 = 11000000

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 Data Encryption Standard (DES) and Fast Encryption Algorithm (FEAL) would transmit the P8 message:

{[11000000][00000110][00000000][00000010][00000000][00000000][00000001][00000000]}

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 = 11000001;

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).

Media identifiers

One byte is used for identifying which elements of the audio-visual 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, 1=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 Frame Alignment Signal (FAS), BAS and ECS) is encrypted. Procedures for other cases are under study.

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 should 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" (see clause A.1);
0 0 0 0 0 0 1 0	"DES" (see clause A.2), Mode 1;
0 0 0 0 0 0 1 1	Reserved for "DES" (see clause A.2), Mode 2;
0 0 0 0 0 1 0 0	Reserved for "DES" (see clause A.2), Mode 3;
0 0 0 0 0 1 0 1	B-CRYPT - ISO/IEC 9979 algorithm Registration No. 0001 [7];
0 0 0 0 0 1 1 0	IDEA - ISO/IEC 9979 algorithm Registration No. 0002 [8];
0 0 0 0 0 1 1 1	BARAS (ETSI) - ISO/IEC 9979 algorithm Registration No. 0011 [10];
other values	Not allocated. Reserved for future use.

BARAS: Baseline Algorithm Recommended for use in Audiovisual Systems
IDEA: International Data Encryption Algorithm

Parameter Identifiers

One byte is used for identifying parameters of the encryption algorithms which are defined in subclause 5.2. Default value is [00000000], which may be used when the algorithm does not need parameter values.

Equipment should 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.

Other messages

P1

Message Name: Cannot Encrypt;

Meaning: The sender of this message will not use an encryption system;

Message Identifier: 1 0 P t_1 t_2 t_3 t_4 t_5 = 10000001;

Content: This message has no content.

P2

Message Name: Failure to start encryption system;

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;

Message Identifier: 1 0 P t_1 t_2 t_3 t_4 t_5 = 10000010;

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.

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
1000 0000 1110 0100 0000 0111 0010 0000 1010 0001 0000 0101 0000 1000 1011 0000 0100 1100 0000 0010 0110 0000 0001 0011	1110 0111 1010 0101 1011 1100 0110 0011 1000 0100 0010 0001

Figure 3: Error correction matrices

5.2 Transmission encryption method

This subclause 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 Cyclic Redundancy Check 4 (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 re-synchronizing 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 re-synchronization is obtained.

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

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

b) cipher stream is generated, but not applied: FAS and BAS in initial and additional channels (see ITU-T Recommendation H.221 [2]) 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 ITU-T Recommendation H.221 [2], annex 2, cipher stream is generated for the eighth sub-channel 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.

The Parameter Identifier is set to [00000000] as default if not otherwise specified.

For the operational parameters for each encryption method to be used, refer to annex C.

5.3 Procedure for use of the system

When a terminal wishes to start encryption, having received the capability "encryp." (see ITU-T Recommendation H.221 [2]) in the capset of the remote terminal, it opens the ECS channel and transmits message(s) P8. On receipt 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, and then begins the transmission of IV blocks. Examples of complete procedures for an encryption session are presented in annex C.

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

6 Encryption of MLP channel

For further study.

Annex A (normative): Encryption algorithms and their parameters

A.1 BARAS

BARAS is a cryptographic algorithm which has been designed by ETSI specifically and exclusively for providing confidentiality for audio-visual services as specified in this ETS. The Parameter Identifier for BARAS is set to [00000000]. The specification of BARAS may be obtained from the ETSI appointed custodian whose co-ordinates are given below. The algorithm may be requested by any organizational manufacturing audio-visual terminals which conform to this ETS. It will be provided subject to a confidentiality and restricted usage undertaking.

The BARAS custodian:

ETSI
Mr. Pierre de Courcel
Fax: +33 4 93 65 47 16

A.2 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 ISO/IEC 9979 Registration No. 0002 [8] (IDEA).

The mode of operation to produce the cipher stream is Output Feedback 8 (OFB-8) according to ISO/IEC 8372 [13]. The Starting Variable (SV) 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/IEC 8372 [13]. 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 ISO/IEC 9979 Registration No. 0002 [8] (IDEA).

The Parameter Identifier is set to [0000 0000] in this mode.

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/IEC 8372 [13]. Details of FEAL algorithm are given in ISO/IEC 9979 Registration No. 0002 [8] (IDEA). 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. See figure A.1.

The SV is identical to 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 audio-visual 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.

The Parameter Identifier is set to [00000000].

A.4 DES

The DES algorithm and the methods of applying the cipher stream to the data stream are described in ISO/IEC 9979 Registration No. 0010 [9] (FEAL).

DES Mode 1 uses one of the two methods designated OFB-8 and OFB-64. The SV is identical to the IV. The Parameter Identifier is set as follows:

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

All other values of the Parameter Identifier are reserved for further study.

DES Mode 2 and DES Mode 3 are for further study.

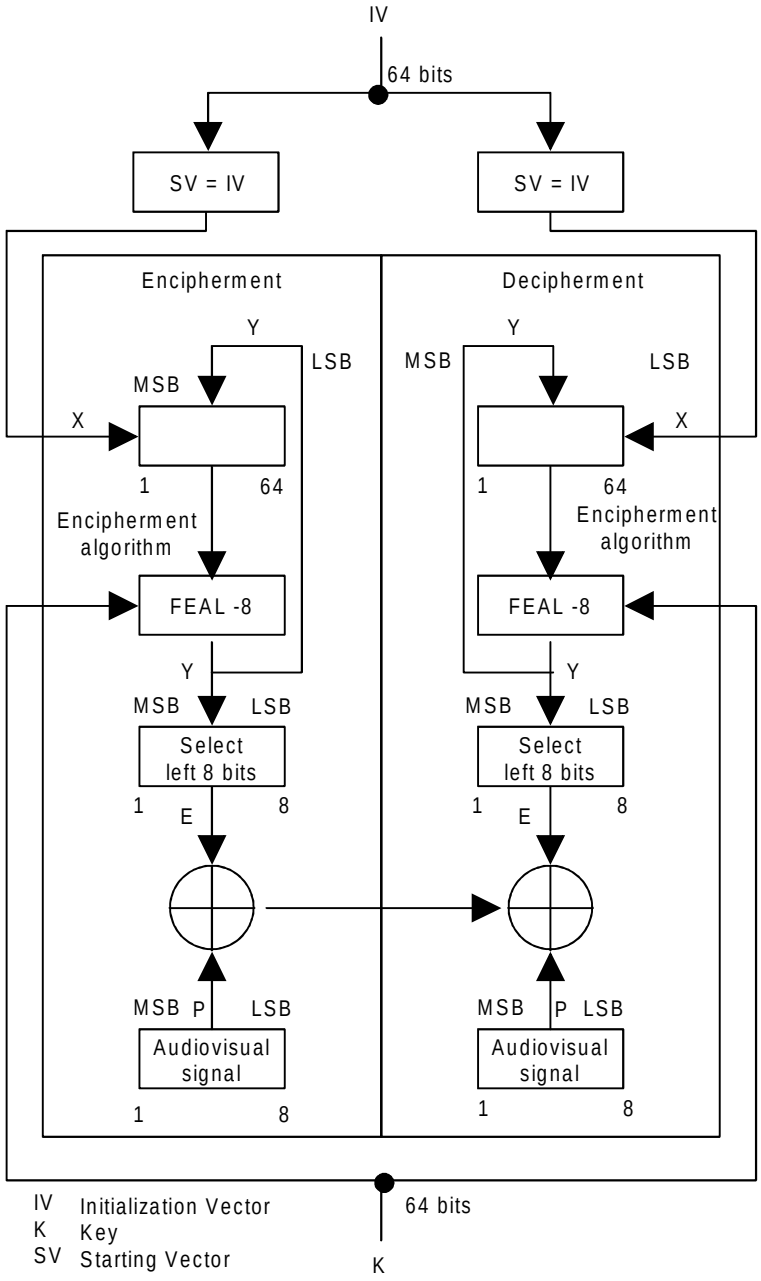


Figure A.1: Output feedback (OFB) mode operation for FEAL

Annex B (informative): Encryption and decryption for 2 × B channels

This annex 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.

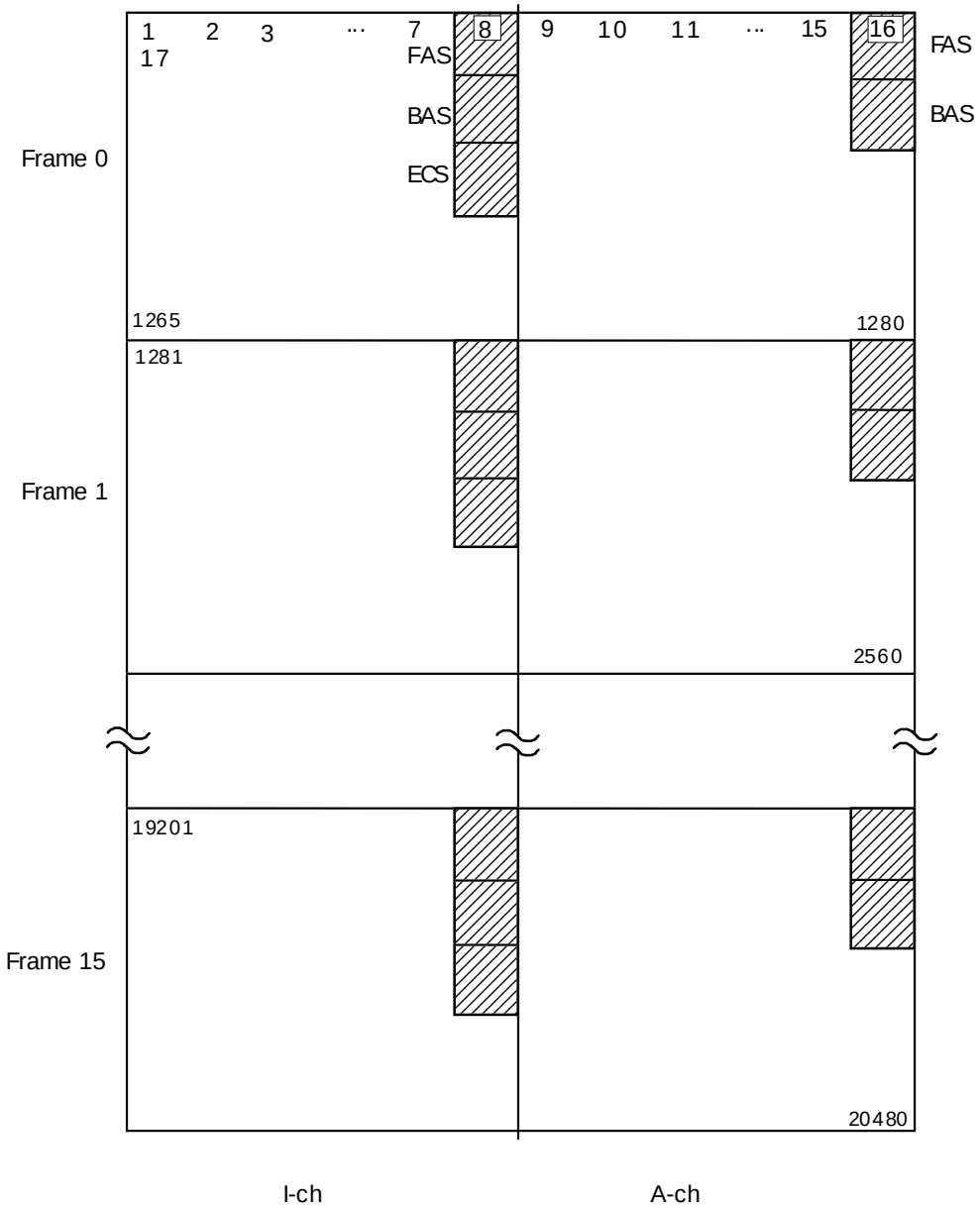
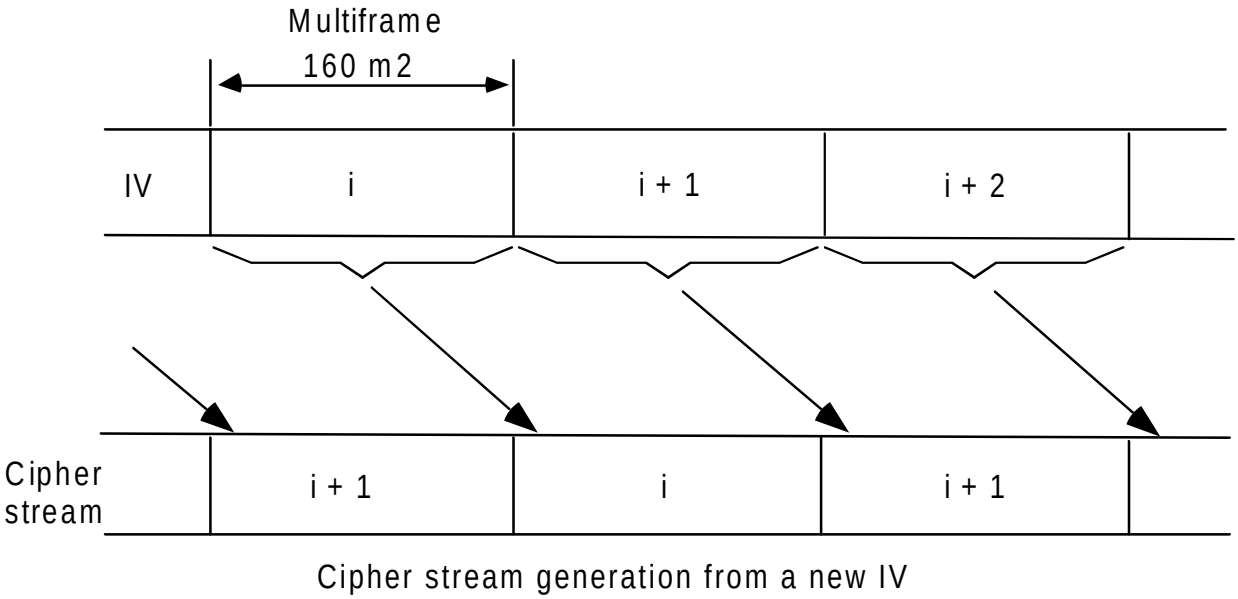


Figure B.1: Bit numbering and unenciphered bits in a multiframe for 2 × B channel



Cipher stream generation from a new IV

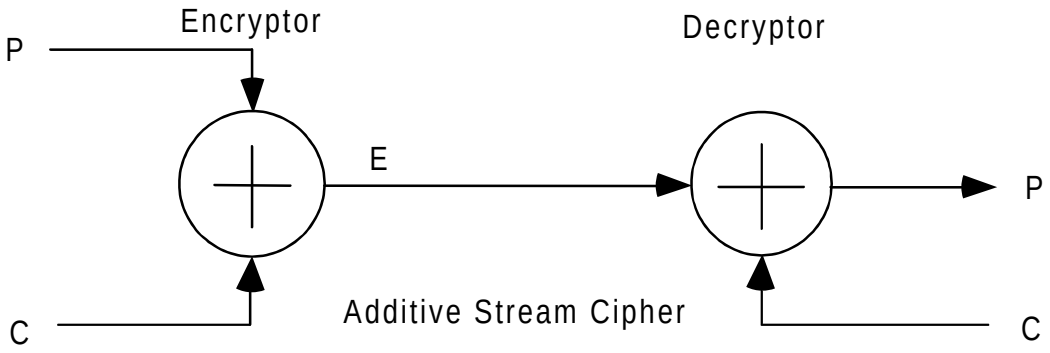
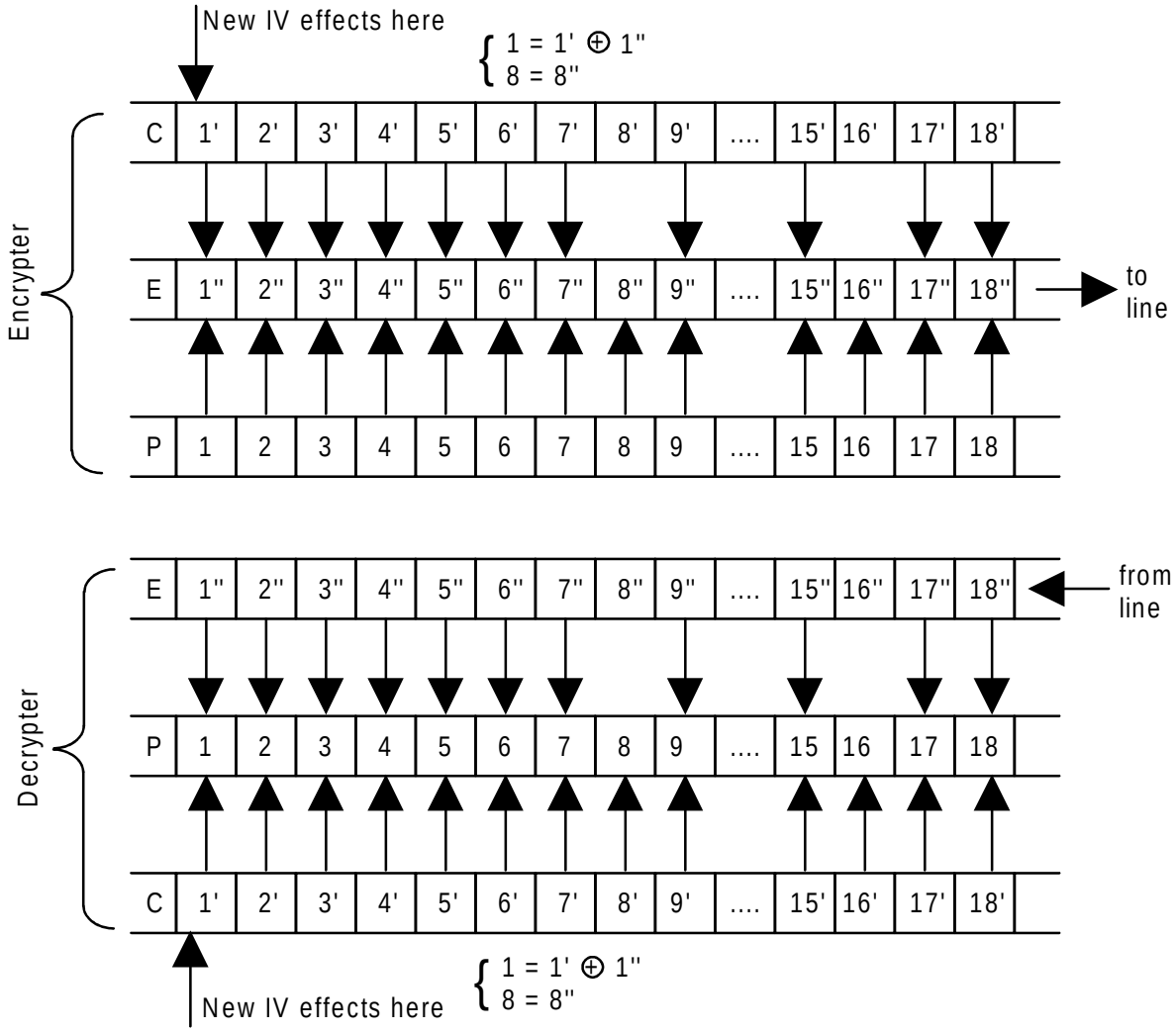


Figure B.2



P Plain text
C Cipher stream
E Encrypted text

Figure B.3

Annex C (informative): Audio-visual privacy communication procedure

When privacy is required in an audio-visual communication session, it is achieved by applying ITU-T Recommendations H.233 [1], H.234 [4] and other H-series recommendations. Since necessary elements of communication procedures are defined in several recommendations, this annex provides examples for a set of procedures with reference to those recommendations.

There may be two scenarios for starting privacy in an audio-visual 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 audio-visual communication happens until the confidentiality mechanism is fully operational.

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

When privacy communication is invoked, particular attention should be paid to the timing when the audio-visual 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 encrypted communication until the encrypted signals become available (scenario 1 above), or another way may be to totally mute audio-visual 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 C.1: Case of privacy being invoked after the call set-up

Time order	Procedure	Message	Channel used	Reference
1	Call set-up	BC/LLC/HLC	D-channel	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	H.230
3	ECS Capability exchange (note 1)	Encrypt-cap	BAS	H.242
4	Opening of ECS channel (note 1)	Encrypt-on	BAS	H.242
5	Identification of available encryption algorithms	P8	H.233	
6	Identification of common key management systems	P0	ECS(SE)	H.234
7	Key management method is known, choose encryption algorithm	-	(Local)	
8	Send the chosen algorithm for both of session key exchange and audio-visual communications	P9		H.233
9	Exchange of prime, primitive root and intermediate result	P3,P4	ECS(SE)	H.234
10	Calculation of *key*;rl,r2 and R12	-	(Local)	H.234
11	Presentation of 64 bit check code as 16 hexadecimal digits	(local)	(Local)	H.234
12	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)	H.234
13	Transmission of initialization vector and 4N bits encrypted random number	P6	ECS(SE)	H.234 (note 3)
14	Encryption on, and initialization vector	A and IV in ECS	ECS(IV)	H.233
15	Indicate outgoing encrypted; unmute, if not automatic; verbal check if required and not already done	- AIA 16 hex digits	(Local) BAS Main channel	H.230 H.234
16	Encrypted audio-visual communications	Audio, video, etc.	Main channel	
17	Mute audio, suppress video	AIM, VIS	BAS	H.230
18	Encryption off	A in ECS	ECS(IV)	H.233
19	Closing of ECS channel (note 4)	Encrypt-off	BAS	H.242
20	Call clear down	-	D-channel	Q.939

NOTE 1: As part of the mode initialization and common mode establishment phase procedures defined in ITU-T Recommendation H.242 [5].

NOTE 2: The encryption algorithm and mode described in annex A of this ETS are commonly used for both session key exchange and audio-visual 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 Recommendation H.242 [5].

Table C.2: Case of privacy being decided before the call set-up

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

NOTE 3: The encryption algorithm and mode described in annex A of this ETS are commonly used for both session key exchange and audio-visual 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 Recommendation H.242 [5].

History

Document history			
January 1997	Public Enquiry	PE 9722:	1997-01-31 to 1997-05-30
August 1997	Vote	V 9742:	1997-08-19 to 1997-10-17