SLOVENSKI STANDARD
SIST ETS 300 840 E1:2003

01-december-2003

Telekomunikacijska varnost – Digitalno omrežje z integriranimi storitvami (ISDN) – Sistem zaupnosti pri avdiovizualnih storitvah

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

Ta slovenski standard je istoveten z: **ETS 300 840 Edition 1**

ICS:

33.080	Digitalno omrežje z integriranimi storitvami (ISDN)	Integrated Services Digital Network (ISDN)
33.160.01	Avdio, video in avdiovizualni sistemi na splošno	Audio, video and audiovisual systems in general

SIST ETS 300 840 E1:2003 **en**

EUROPEAN TELECOMMUNICATION STANDARD

ETS 300 840

January 1998

Source: 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

Foreword 5

1 Scope 7

2 Normative references 7

3 Abbreviations 8

4 Properties of the system specified 8
4.1 Confidentiality 8
4.2 Algorithm specification 8

5 The confidentiality mechanism 9
5.1 Description of operation 9
5.1.1 Controls and indication within the H.221 frame 9
5.1.2 Message formats 10
5.1.2.1 Identifier 10
5.1.2.2 Length (L) 10
5.1.2.3 Bit string 10
5.1.3 Unenciphered ECS channel 11
5.1.3.1 Session exchange blocks 12
5.1.3.2 Initialization vectors 14
5.1.3.3 Error protection of control channel information 14
5.2 Transmission encryption method 14
5.3 Procedure for use of the system 15

6 Encryption of MLP channel 15

Annex A (normative): Encryption algorithms and their parameters 16

A.1 BARAS 16

A.2 IDEA 16

A.3 FEAL 16

A.4 DES 17

Annex B (informative): Encryption and decryption for 2 × B channels 18

Annex C (informative): Audio-visual privacy communication procedure 21

History 24

Blank page

Foreword

This European Telecommunication Standard (ETS) has been produced by the Security (SEC) Technical Committee of the European Telecommunications Standards Institute (ETSI).

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.

Transposition dates	
Date of adoption of this ETS:	24 October 1997
Date of latest announcement of this ETS (doa):	30 April 1998
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	31 October 1998
Date of withdrawal of any conflicting National Standard (dow):	31 October 1998

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.

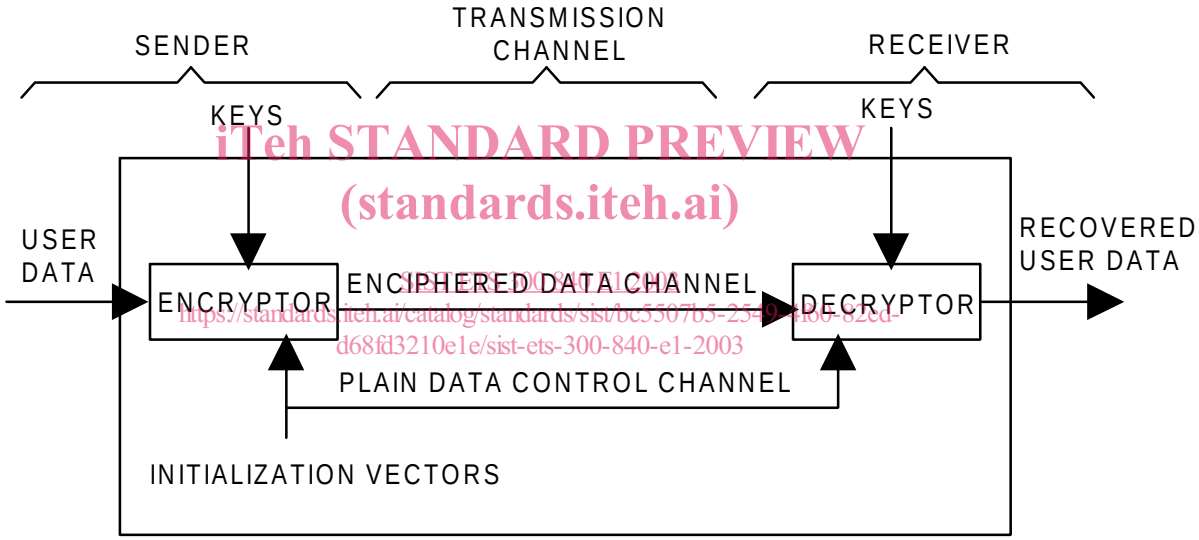

Figure 1: Block diagram of the link encryption system

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.