SLOVENSKI STANDARD
SIST ETS 300 841 E1:2003

01-december-2003

Telekomunikacijska varnost ï Digitalno omreģje z integriranimi storitvami (ISDN) ï Sistem za upravljanje in avtentikacijo s ključ em za ģifriranje pri avdiovizualnih storitvah

Telecommunications security; Integrated Services Digital Network (ISDN); Encryption key management and authentication system for audiovisual services

Ta slovenski standard je istoveten z: **ETS 300 841 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 300 841 E1:2003 **en**

EUROPEAN TELECOMMUNICATION STANDARD

ETS 300 841

January 1998

Source: Security

Reference: DE/SEC-002309

ICS: 33.020

Key words: ISDN, multimedia, security

Telecommunications Security; Integrated Services Digital Network (ISDN); Encryption key management and authentication 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

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

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.234 [1] and describes authentication and key management methods for a privacy system suitable for use in narrowband audiovisual services conforming to ITU-T Recommendations H.221 [5], H.230 [6] and H.242 [8]. The confidentiality specification is independent, and is contained in the separate ITU-T Recommendation H.233 [7].

Privacy is achieved by the use of secret keys. The keys are loaded into the confidentiality part of the privacy system and control the way in which the transmitted data is encrypted and decrypted. If a third party gains access to the keys being used then the privacy system is no longer secure.

The maintenance of keys by users is thus an important part of any privacy system. Three alternative practical methods of key management are specified in this ETS. For cases where automated key management is not feasible, an unspecified alternative such as manual key management can be used.

The first is identified as ISO 8732 [2]. It is based on manually installed keys in systems that physically afford those keys a high measure of protection, and then an automated exchange of keys encrypted under the manually distributed keys. The algorithm used for encrypting these automatically distributed keys is normally the same as that used for encrypting the communication itself. The security of automatically distributed keys depends on the security of the manually distributed keys.

Automatically distributed keys may be used for a single session, or may be used for multiple sessions in a given period of time (e.g., a month). ISO 8732 [2] contains protocols not only for the automated exchange of information between the two terminals, but also physical protocols for ensuring the security of the manual distribution of keys as well.

There are two distinct environments: direct point-to-point (two layer), where the two terminals share a common key, and, a three-layer environment, where the two terminals who wish to communicate do not share a common key, but use the facilities of a mutual third party, with whom each of them do share a common key. The interfaces to the third party are outside this ETS, although it is required to distinguish between the two environments.

NOTE 1: Session key exchange specified in subclause 5.3.2 is functionally duplicated in ANSI X.9.17 [3], in that the keys automatically distributed in ANSI X.9.17 [3] are strong enough to be used as session keys. However, to follow the form of this recommendation, these keys are referred to as *key* in subclause 5.3.2.

The second is a simple yet secure method known as "extended Diffie-Hellman", which generates and exchanges keys automatically via the system itself (this key exchange is itself encrypted). It requires no action from users until keys have been exchanged; they are then advised to confirm verbally that the same check sequence is available at each terminal. The method is quite adequate to prevent outsiders listening in on an audiovisual call carried over a satellite channel, for example. To defeat the system, it would be necessary for the interloper to intercept totally the bi-directional communication before encryption had been activated, and to exchange keys with both parties, pretending to each that it is the other legitimate party. The method does not provide authentication.

The third method is again more complex and provides a higher degree of privacy and also provides authentication of audiovisual service entities (terminals, Multi-point Control Units (MCUs), etc.). The public key cryptosystem invented by Rivest, Shamir and Adleman ("the RSA method") is very similar to the public key method specified in ITU-T Recommendation X.509 [9] and uses the RSA algorithm. The method requires the establishment of a security agency, available to the whole population of entities which require interconnectability: certification is effectively "off-line", and relies on the integrity of the agency. This authentication mechanism allows the parties involved in a conference call to be identified to others in an assured manner, and can be operated in multipoint as well as point-to-point calls.

All methods require the use of an associated error-free clear channel.

NOTE 2: Access control, integrity and non-repudiation are not provided by any of these methods.

A fourth method is referred to in this ETS as "manual key exchange".

Manual key exchange is defined as the users entering key encryption keys directly into terminals, without H.KEY message exchanges. The same key is entered at both locations. The length of the keys is dependent on the encryption algorithm. The bit order for the keys is Most Significant Bit (MSB) entered first and Least Significant Bit (LSB) entered last. The actual mechanism for entering the keys into the terminal is terminal dependent and beyond the scope of this ETS.

Examples are given below:

- use a telephone keypad to enter: (MSB) 00111010...01110100 (LSB);
- download the same from a computer;
- use a keyboard to enter the same as hexadecimal characters: (MSB) 3A...74 (LSB).

Manual entry may occur prior to initiating the call, or while in a call. In the latter case, the parties may decide to invoke encryption while in a conference, enter a key using the interface provided by the terminal, and then initiate encryption through the terminal's user interface. It is when encryption is requested through the user interface that the Bit-rate Allocation Signal (BAS) code "Encrypt-On" is sent, the Encryption Control Signal (ECS) channel is opened, encryption algorithms are selected, manual mode of key management is agreed to, and session keys are exchanged.

For an encryption system to be regarded as private all conferees should be aware of who/what has access to unencrypted data, whether other conferees or equipments such as MCUs or conversion facilities. This requires an initial set-up period before a conference starts so that entities can authenticate each other. Thus all entities that have access to unencrypted data are identified in an assured manner to all other entities before the conference commences. The authentication framework also provides information to any network provider, for example billing information for an MCU call.

If unencrypted data is available at the MCU (a so-called "trusted MCU") the equipment should be part of any authentication framework. Users should also be made aware that there is a trusted MCU in the network.

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.234: "Key Management Procedures".

[2] ISO 8732: "Banking Key Management".

[3] ANSI X.9.17: "Financial Institution Key Management".

[4] ITU-T Recommendation X.209: "Specification of basic encoding rules for Abstract Syntax Notation One (ASN.1)".

[5] ITU-T Recommendation H.221: "Frame structure for a 64 to 1 920 kbit/s channel in audiovisual teleservices".

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

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

NOTE: ITU-T Recommendation H.233 forms the basis of ETS 300 840 [10].

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

[9] ITU-T Recommendation X.509: "The directory-authentication framework".

[10] ETS 300 840: "Telecommunications Security; Integrated Services Digital Network (ISDN); Confidentiality system for audiovisual services".

[11] ITU-T Recommendation T.120: "Data protocols for multimedia conferencing".

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

3 Definition

For the purposes of this ETS, the following definition applies:

***key*:** key-encrypting key

4 Abbreviations

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

ANSI	American National Standards Institute
ASN.1	Abstract Syntax Notation 1 (see ITU-T Recommendation X.209 [4])
AVSE	AudioVisual Service Entity (terminals, MCUs, etc.)
BAS	Bit-rate Allocation Signal
CA	Certification Authority
CCA	Country Certification Authority
CKD	Key Distribution Centre
CKT	Key Translation Centre
CSM	Cryptographic Service Message
DES	Data Encryption Standard
DSM	Disconnected Service Message
ECS	Encryption Control Signal
ExOR	Exclusive-OR (logical operator)
GCA	General Certification Authority
ILC	Identifier, Length, Content
KSM	Key Service Message
LSB	Least Significant Bit
MCU	Multi-point Control Unit
MLP	Multi-Layer Protocol
MSB	Most Significant Bit
RSA	public key cryptosystem invented by Rivest, Shamir and Adleman
RSM	Response Service Message
SE	Session Exchange

5 Message system and key exchange

5.1 Message channel

The system described below consists of a number of defined messages conveyed in sequence between the two ends of the link. The error-free channel required for this purpose is described in ITU-T Recommendation H.233 [7], where reference is made to Session Exchange (SE) blocks.

5.2 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.209 [4]. The length may be encoded in short form or long form. The indefinite form as defined in ITU-T Recommendation X.209 [4] will not be used.

The messages described in this ETS 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 ETS.

A short description of some of the ITU-T Recommendation X.209 [4] definitions used within this ETS is given in subclauses 5.2.1 to 5.2.3.

5.2.1 Identifier

An identifier is an octet with the structure shown in figure 1.

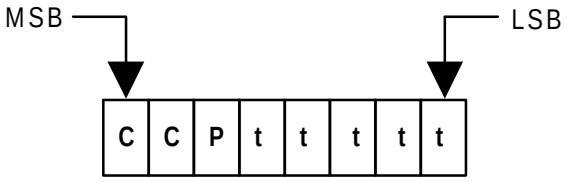

Figure 1

The two bits CC, "Tag Class", define the type of identifier: this is 10 (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 (ttttt) uniquely defines the identifier (according to its class).

Therefore, all identifiers in this ETS have the octet form: 1 0 P t_1 t_2 t_3 t_4 t_5.

5.2.2 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 $2^{1\,008}$. 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.

5.2.3 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.