SLOVENSKI STANDARD
SIST EN 301 132 V1.1.1:2003

01-december-2003

Digitalno omrežje z integriranimi storitvami (ISDN) – Varnostna orodja (SET) za uporabo v telekomunikacijskih storitvah

Integrated Services Digital Network (ISDN); Security tools (SET) for use within telecommunication services

Ta slovenski standard je istoveten z: EN 301 132 Version 1.1.1

ICS:

33.080	Digitalno omrežje z integriranimi storitvami (ISDN)	Integrated Services Digital Network (ISDN)

SIST EN 301 132 V1.1.1:2003 **en**

EN 301 132 V1.1.1 (1998-10)

European Standard (Telecommunications series)

Integrated Services Digital Network (ISDN); Security tools (SET) for use within telecommunication services

Reference
DEN/NA-020036 (ahc00ico.PDF)

Keywords
ISDN, security

ETSI

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Internet
secretariat@etsi.fr
http://www.etsi.org

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This European Standard (Telecommunications series) has been produced by ETSI Technical Committee Network Aspects (NA).

National transposition dates	
Date of adoption of this EN:	30 October 1998
Date of latest announcement of this EN (doa):	31 January 1999
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 July 1999
Date of withdrawal of any conflicting National Standard (dow):	31 July 1999

1 Scope

The present document is a description of Security Tools (SET) for use within ISDN telecommunication services from the user's point of view. It does not deal with the details of the human interface itself.

NOTE 1: The SETs are in principle application independent. Although they are designed for the use within ISDN, they could be applicable to other networks such as B-ISDN or PSTN depending on the requirements for the telecommunication service to be protected and the service provider's decision.

Charging principles are outside the scope of the present document.

The use of one of the SET helps in providing an appropriate level of security for a given ISDN telecommunication services.

NOTE 2: The present document describes two security tools for the use in ISDN, i.e. Personal Identification Number (PIN) and Transaction Number (TAN). These are intended to be used for the Integrated Services Digital Network (ISDN) Remote Control (RC) service and Outgoing Call Barring – User Controlled (OCB-UC) supplementary service. Due to the increasing demand for enhanced security mechanisms in telecommunication services, more tools may be added in future versions of the standard. Possible candidates for the use within N-ISDN are described in ETR 237 [4].

The present document is applicable to the stage two and stage three standards for the ISDN Security Tools. The terms "stage two" and "stage three" are also defined in CCITT Recommendation I.130 [2]. Where the text indicates the status of a requirement (i.e. as strict command or prohibition, as authorization leaving freedom, as a capability or possibility), this shall be reflected in the text of the relevant stage two and stage three standards.

Furthermore, conformance to the present document is met by conforming to the stage three standards with the field of application appropriate to the equipment being implemented. Therefore, no method of testing is provided for the present document.

2 References

References may be made to:

a) specific versions of publications (identified by date of publication, edition number, version number, etc.), in which case, subsequent revisions to the referenced document do not apply; or

b) all versions up to and including the identified version (identified by "up to and including" before the version identity); or

c) all versions subsequent to and including the identified version (identified by "onwards" following the version identity); or

d) publications without mention of a specific version, in which case the latest version applies.

A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

2.1 Normative references

[1] ITU-T Recommendation I.112 (1993): "Vocabulary of terms for ISDNs".

[2] CCITT Recommendation I.130 (1988): "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".

[3] ETR 232 (1996): "Security Technical Advisory Group (STAG); Glossary of security terminology".

[4] ETR 237 (1996): "Security Technical Advisory Group (STAG); Baseline security standards; Features and mechanisms".

[5] ETR 236 (1996): "Security Technical Advisory Group (STAG); A guide to the ETSI security standards policy".

[6] TCR-TR 49: "Security Technical Advisory Group (STAG); Security requirements capture".

[7] ETS 300 391-1 (1995): "Universal Personal Telecommunication (UPT); Specification of the security architecture for UPT phase 1; Part 1: specification".

2.2 Informative references

None

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following definitions in addition to those contained in ETR 232 [3] apply:

telecommunication service: see ITU-T Recommendation I.112 [1], subclause 2.2, definition 201. In the context of the present document, the term telecommunication service includes basic services, teleservices and supplementary services.

confidential information: the information that is necessary to make use of a SET.

Integrated Services Digital Network (ISDN): see ITU-T Recommendation I.112 [1], subclause 2.3, definition 308.

network operator: the entity which provides the network operating elements and resources for the execution of the Security Tool.

Security Tool (SET): a tool provided in support of the security of a service.

served user: the user to whom a SET is provided to in combination with a telecommunication service.

Transaction Number (TAN): a TAN is a one time password.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

(N)-ISDN	(Narrowband)-Integrated Services Digital Network
B-ISDN	Broadband Integrated Services Digital Network
DTMF	Dual Tone Multi Frequency
OAM	Operation and Maintenance
OCB-UC	Outgoing Call Barring - User ControlledPIN Personal Identification Number
PIN	Personal Identification Number
PSTN	Public Switched Telephone Network
RC	Remote Control
SET	Security tools
TAN	Transaction Number

4 General aspects

4.1 Description

Security Tools are means of providing an appropriate level of security and protection to the user of a given telecommunication service.

In general, security is needed to provide:

- protection of information;
- authenticity;
- availability;
- integrity;
- confidentiality;
- access control;
- non-repudiation.

According to the telecommunication service concerned, the applicability of SET can relate to the basic communication and the following operations of this service:

- activation;
- deactivation;
- registration;
- erasure;
- invocation;
- interrogation.

For the provider of a vulnerable telecommunication service, the selection and the application of a SET in conjunction with that telecommunication services requires careful investigation, whether the chosen SET provides a sufficient level of security to the associated telecommunication service, taking into account, the possible scenarios. The two stage method described in ETR 236 [5] and TCR-TR 49 [6] shall be applied by the service provider when choosing the SETs. The first stage of this process is the security requirements capture stage, including a risk and threat analysis, in the second stage the features and mechanisms, i.e. in ISDN the SETs, are defined.

4.2 Procedures

4.2.1 Provision and withdrawal

A SET is provided and withdrawn as a part of a telecommunication service concerned.

The service provider shall provide the served user with the necessary confidential information to apply the SET.

The way of providing this information is outside the scope of the present document.

NOTE: Service provider and served user shall take the necessary steps to prevent other parties from the unauthorized use of a SET. When the served user provides the confidential information to any other party, the served user is responsible for the misuse of the SET and all its consequences.