Draft EN 301 132 V1.1.1 (1997-12)

European Standard (Telecommunications series)

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

European Telecommunications Standards Institute

Reference
DEN/NA-020036 (ahc00ico.PDF)

Keywords
ISDN, SET

ETSI Secretariat

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

X.400
c= fr; a=atlas; p=etsi; s=secretariat

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

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 ETR 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.fr/ipr).

Pursuant to the ETSI Interim 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 ETR 314 (or the updates on http://www.etsi.fr/ipr) which are, or may be, or may become, essential to the present document.

Foreword

This European Standard (telecommunication series) has been produced by the Network Aspects (NA) Technical Committee of the European Telecommunications Standards Institute (ETSI), and is now submitted for the Public Enquiry phase of the ETSI standards Two-step Approval Procedure.

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

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 current version of this ETS 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) and Outgoing Calls Barred within CUG (OCB) supplementary services. Due to the increasing demand for enhanced security mechanisms in telecommunication services, more tools may be added in future versions of the present document. 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 [8]. 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.

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

[2] DE/NA-020012: "Charge Card Calling (CCC) Service description", Version 7 Revised 1, 07 September 1994".

[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 049:"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".

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

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] shall apply.

telecommunications service: See ITU-T Recommendation I.112 [1], paragraph 2.2, definition 201. In the context of this ETS, 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 Recommendation I.112 [1], paragraph 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	Outgoing Calls Barred within the CUG
PIN	Personal Identification Number
PSTN	Public Switched Telecommunication Networks
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 telecommuncation service, taking into account, the possible scenarios. The two stage method described in ETR 236 [5] and TCR-TR 049 [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.

4.2.2 Activation, deactivation and registration

The SET is part of the telecommunication service making use of it. One SET can be related to several telecommunication services subscribed to by the served user.

One confidential information may relate to several telecommunication services. As a service provider option, it may be possible to provide several sets of confidential information, relating to several telecommunication services.

The confidential information associated with the SET is registrated by the service provider at provision. If the served user subscribes to a new telecommunication service that needs a security procedure or if the served user has the possibility to modify the parameters of the SET, the served user can indicate to the service provider which SETs are given. Then the service provider shall update the registration data associated to this SET.

For each SET provided, the following data shall be registrated by the service provider:

- Type of SET: (e.g. PIN, TAN);
- value of the SET parameter (i.e. password);
- the list of the telecommunication services associated (e.g.: RC: remote control service, OCB: outgoing call barring-user controlled supplementary service).

The handling of the SET, e.g. inserting the confidential information before or after putting in the telecommunication service code, is a service provider option.

4.2.3 Erasure

See the following appropriate procedures of the SETs in clause 6.

4.2.4 Invocation and operation

Invocation of the SET shall occur in association with the relevant operation on the telecommunication service concerned. The result of the invocation shall be transmitted to that telecommunication service.

4.2.5 Interrogation

Not applicable.

4.3 Intercommunication considerations

Intercommunication across several networks shall be possible. Individual interactions are described within the various telecommunication services.

5 Security Tools (SET)

5.1 Personal Identification Number (PIN)

5.1.1 Description

The principles of the authentication using PINs is described in ETR 237 [4]. In ISDN, the PIN is used when accessing a telecommunication service to ensure that this service is used with an appropriate level of security.

The determination of the maximum number of the alphanumerical characters of the PIN is a service provider option. However, the lower limit is 4, the maximum number is 12.

The served user shall have the possibility to change the PIN at any time after the initial provision.

During the operation of the service, the user shall be informed (visually or, in the case of PSTN, by announcements) when he is expected to enter the PIN and when validation was unsuccessful. Also, he shall be informed of the result of the operations when e.g. changing his PIN:

5.1.2 Provision and withdrawal

The PIN shall be provided in connection with the provision of given telecommunication services (e.g. OCB: outgoing call barring-user controlled supplementary service).

The procedure for the generation, provision and withdrawal of the use of the PIN is outside the scope of the present document.

5.1.3 Normal procedures

5.1.3.1 Registration and erasure

The initial registration procedure is done by the service provider as a part of the provision. It shall be possible for the served user to change the PIN with a user procedure after the initial registration.

Change of the current PIN is performed by using a registration procedure. A successful registration procedure consists of:

- entering of the old PIN, then
- entering of the new PIN, then
- one repetitive entering of the new PIN
    - validation of all PINs;
    - replacement of the old PIN in the network (overwriting) by the new PIN after checking the old, the new and the repetive new PIN by the network.

NOTE: The served user may be requested to change the PIN periodically. This is an administrative matter between the served user and the service provider. When the current PIN expires, the service provider marks the PIN as such in his network using an Operation and Maintenance (OAM) procedure.

Primitive PlNs with an easy combination of characters (e.g. "1234" or "2221") shall be rejected by the network.

The definition of primitive PINs is a service provider option.

For the reason that the served user does not always need to use a PIN, the registration should be possible independent from the following parameters:

- the kind of supplementary service or service;
- security level;
- date and time of activation and deactivation;
- duration of activation and deactivation;
- amount of transferred data volume, length, etc.

With the registration of the new PIN the old one is automatically overwritten (i.e. erased).

5.1.3.2 Activation, deactivation

Not applicable.

5.1.3.3 Invocation and operation

See subclause 4.2.4.

5.1.3.4 Interrogation

Not applicable.

5.1.4 Exceptional procedures

5.1.4.1 Activation, deactivation and registration

Activation and deactivation: not applicable.

Unsuccessful registration (i. e; for modification of a PIN) occurs in the following conditions:

- telecommunication service using the SET "PIN" not provided (not subscribed to by the served user);
- invalid or incorrect PIN;
- invalid new PIN;
- new PIN being identical to the old one;
- new primitive PIN;
- incorrect repetition of the new PIN;
- registration blocked.

If whilst changing the PIN the new PIN is not entered a second time, as required, and/or validation has not been successful, the registration procedure is considered as cancelled, the previous PIN is still applicable.

During the registration procedure, the number of attempts using an incorrect PIN (i.e. old PIN) shall be checked by the network. In the case of N successive unsuccessful attempts, the registration procedure is blocked. The value of N is a service provider option, but shall be 3 at minimum.

Reinitialization of the value of N to zero shall occur in the case where a correct PIN is entered if the registration procedure is not blocked.

As a service provider option, the served user may receive an indication whether somebody has tried to change the PIN or to access the protected telecommunication service and entered wrong PINs N-X times without completing the authentication procedure.

The served user having his/her registration operation blocked, shall be able to request reinitialization of the telecommunication service using the SET "PIN" by the service provider. This is an administrative matter and outside the scope of this ETS.

If the served user does not change the PIN when requested (e.g. periodically), the related telecommunication service shall be blocked.

5.1.4.2 Erasure

Not applicable.

5.1.4.3 Invocation and operation

Unsuccessful invocation associated with a telecommunication service occurs in the following conditions:

- invalid or incorrect PIN;
- telecommunication service using SET "PIN" is blocked.

The number of attempts based on the use of an incorrect or invalid PIN shall be checked by the network. In the case of N successive unsuccessful attempts, the telecommunication service using the SET "PIN" is blocked.

The value of N is a service provider option, but shall be 3 at minimum. Reinitialization of the value of N to zero shall occur in the case where a successful invocation attempt is made while the authentication procedure using PIN is not blocked.

The served user having the SET blocked, shall be able to request reinitialization of the telecommunication service using the SET "PIN" by the service provider. This is an administrative matter and outside the scope of this present document.

It is a service provider option to reinitialize the SETautomatically after a predefined time period with a minimum of 24 hours.

As a service provider option, the served user, when invoking the SET the next time, may receive an indication whether in the meantime somebody has tried to change the PIN or to access the protected telecommunication service and entered wrong PINs N-X times.

5.1.4.4 Interrogation

See subclause 4.2.5.

5.2 Transaction Number (TAN)

5.2.1 Description

The TAN is a one time password. In ISDN, the TAN is used usually together with a PIN when accessing a telecommunication service to ensure that this service is used with an appropriate level of security.

Each TAN is a combination of at least six alphanumerical characters up to a maximum of 12 alphanumerical characters. Each subscriber receives a list of TANs at subscription time from the service provider. The list of TANs contains a number (e.g. 100) of randomly generated TANs. The length of the TAN is a service provider option, but shall be in the range of 6 to 12. The amount of TANs on the list is outside the scope of the present document.

Another method to provide the TANs to the user is by means of an electronic device which generates automatically the next TAN. The algorithm for calculating the TANs in the device and the network needs to be the same. The user is required to enter the TAN provided by the device into the terminal for accessing the associated telecommunication service.

NOTE: In some cases the result of the dynamic calculation may be transferred directly by this device via the terminal to the network using DTMF signalling, as described, for instance, in ETS 300 391-1 [7].

During each authentication procedure for the specific telecommunication service requiring the SET "TAN", each TAN must be used in sequence and once only from the list, until all TANs have been exhausted.

When the list of TANs is almost used up, on the subscribers request or on the service providers decision, the subscriber shall receive a new list of TANs.

5.2.2 Provision and withdrawal

The list of TANs shall be provided in connection with the provision of certain telecommunication service (e. g. Remote control supplementary service).

The procedure for the generation, provision and withdrawal of the list of the TAN is outside the scope of the present document.

The valid TANs are automatically activated at provision.

5.2.3 Procedures

5.2.3.1 Activation, deactivation and registration

Modification of the TANs on the current list of TANs shall not be possible.

The TANs on the list of TANs is automatically registered by the service provider when that list is provided to the subscriber.

5.2.3.2 Erasure

If a TAN has been used, it is erased automatically.

The served user has to know which TAN is the next one to be used on the list.

The remaining TANs on the list shall be erased by the service provider on the request of the subscriber.

If the user receives a new list of TANs by the service provider, the remaining TANs of previous list shall be automatically erased.

5.2.3.3 Invocation and operation

The user shall be informed (visually or by announcements) when he is expected to enter the TAN and possibly the PIN. The SET "TAN" is invoked when the TAN is entered.

5.2.3.4 Interrogation

See subclause 4.2.5.

5.2.4 Exceptional procedures

5.2.4.1 Activation, deactivation and registration

Activation, deactivation and registration: Not applicable.

5.2.4.2 Erasure

Not applicable.

5.2.4.3 Invocation and operation

As a service provider option, number of attempts based on the use of an incorrect TAN may be checked by the network. In the case of M successive unsuccessful attempts, the telecommunication service using TAN is blocked. The value of M is a service provider option, but should be "M = 3" at minimum. The procedures associated with this situation conform to subclause 5.1.4.3.

Reinitialization of the value of M to zero shall occur in the case where a successful invocation attempt is made while the SETusing TAN is not blocked.

The served user having the SET blocked, shall be able to request reinitialization of the SET by the service provider. This is an administrative matter and outside the scope of this ETS.

As a service provider option, if an incorrect TAN is used M-X times and the authentication procedure not completed, the served user may be informed by the network accordingly.

Unsuccessful invocation associated with a supplementary service occurs when the TAN is invalid or incorrect.

It is a service provider option to reinitialize the SETautomatically after a predefined time period with a minimum of 24 hours.

5.2.4.4 Interrogation

See subclause 4.2.5.

History

Document history				
V1.1.1	December 1997	Public Enquiry	PE 9817:	1997-12-26 to 1998-04-24