Draft EN 301 002-1 V1.1.1 (1997-12)

European Standard (Telecommunications series)

Integrated Services Digital Network (ISDN); Security tools (SET) procedures; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification

European Telecommunications Standards Institute

Reference
DEN/SPS-05123-1 (9a090ico.PDF)

Keywords
ISDN, DSS1, supplementary service, 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 (Telecommunications series) has been produced by ETSI Technical Committee Signalling Protocols and Switching (SPS), and is now submitted for the Public Enquiry phase of the ETSI standards Two-step Approval Procedure (TAP).

The present document is part 1 of a multi-part standard covering the Digital Subscriber Signalling System No. one (DSS1) protocol specification for the Integrated Services Digital Network (ISDN) Security tools (SET) procedures, as described below:

Part 1: "Protocol specification";

Part 2: "Protocol Implementation Conformance Statement (PICS) proforma specification";

Part 3: "Test Suite Structure and Test Purposes (TSS&TP) specification for the user";

Part 4: "Abstract Test Suite (ATS) and partial Protocol Implementation eXtra Information for Testing (PIXIT) proforma specification for the user";

Part 5: "TSS&TP specification for the network";

Part 6: "ATS and partial PIXIT proforma specification for the network".

In accordance with CCITT Recommendation I.130, the following three level structure is used to describe the supplementary telecommunication services as provided by European public telecommunications operators under the pan-European ISDN:

- Stage 1: is an overall service description, from the user's standpoint;
- Stage 2: identifies the functional capabilities and information flows needed to support the service described in stage 1; and
- Stage 3: defines the signalling system protocols and switching functions needed to implement the service described in stage 1.

The present document details the stage 3 aspects (signalling system protocols and switching functions) needed to support the SET procedures. The stage 1 aspects are detailed in EN 301 132.

NOTE: Currently no stage 2 document exists.

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

This first part of EN 300 002 specifies the stage three of the Security tools (SET) procedures for the pan-European Integrated Services Digital Network (ISDN) as provided by the European public telecommunications operators at the T reference point or coincident S and T reference point (as defined in ITU-T Recommendation I.411 [2]) by means of the Digital Subscriber Signalling System No. one (DSS1) protocol. Stage three identifies the protocol procedures and switching functions needed to support a telecommunications service (see CCITT Recommendation I.130 [10]).

In addition, the present document specifies the protocol requirements at the T reference point where the service is provided to the user via an intermediate private ISDN.

The present document does not specify the additional protocol requirements where the service is provided to the user via a telecommunications network that is not an ISDN.

The SET procedures are a means of providing an appropriate level of security and protection to the user of a given telecommunication service.

Further parts of the present document specify the method of testing required to identify conformance to the present document.

The present document is applicable to equipment supporting the SET procedures, to be attached at either side of a T reference point or coincident S and T reference point when used as an access to the public ISDN.

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] EN 300 196-1 (V1.2): "Integrated Services Digital Network (ISDN); Generic functional protocol for the support of supplementary services; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

[2] ITU-T Recommendation I.411 (1993): "ISDN user-network interfaces - Reference configurations".

[3] CCITT Recommendation X.208 (1988): "Specification of Abstract Syntax Notation One (ASN.1)".

[4] CCITT Recommendation X.219 (1988): "Remote operations: Model, notation and service definition".

[5] ITU-T Recommendation Z.100 (1993): "Specification and Description Language (SDL)".

2.2 Informative references

[6] EN 301 132: "Integrated Services Digital Network (ISDN); Security Tools for use within telecommunication services".

[7] ETR 232 (1995): "Security Techniques Advisory Group (STAG); Glossary of security terminology".

[8] CCITT Recommendation E.164 (1991): "Numbering plan for the ISDN era".

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

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

[11] ITU-T Recommendation I.210 (1993): "Principles of telecommunication services supported by an ISDN and the means used to describe them".

3 Definitions

The following definitions apply:

Integrated Services Digital Network (ISDN): See ITU-T Recommendation I.112 [9], definition 308.

ISDN number: A number conforming to the numbering plan and structure specified in CCITT Recommendation E.164 [8].

invoke component: See EN 300 196-1 [1], subclause 8.2.2.1. Where reference is made to a "xxxx" invoke component, an invoke component is meant with its operation value set to the value of the operation "xxxx".

network: The DSS1 protocol entity at the network side of the user-network interface.

Personal Identification Number (PIN): See ETR 232 [7].

reject component: See EN 300 196-1 [1], subclause 8.2.2.4.

return error component: See EN 300 196-1 [1], subclause 8.2.2.3. Where reference is made to a "xxxx" return error component, a return error component is meant which is related to a "xxxx" invoke component.

return result component: See EN 300 196-1 [1], subclause 8.2.2.2. Where reference is made to a "xxxx" return result component, a return result component is meant which is related to a "xxxx" invoke component.

security tool: See EN 301 132 [6], clause 3.

served user: The user to whom the SET procedures are provided in combination with a telecommunication service.

service; telecommunication service: See ITU-T Recommendation I.112 [9], definition 201.

supplementary service: See ITU-T Recommendation I.210 [11], subclause 2.4.

user: The DSS1 protocol entity at the user side of the user-network interface.

4 Abbreviations

The following abbreviations apply:

ASN.1	Abstract Syntax Notation one
DSS1	Digital Subscriber Signalling System No. one
ISDN	Integrated Services Digital Network
OAM	Operation And Maintenance
PIN	Personal Identification Number
SDL	Specification and Description Language
SET	Security Tools

5 Description

The SET procedures allow a served user to be provided with a PIN. The PIN is used when accessing a telecommunication service to ensure that this service is used with an appropriate level of security. The served user can change the PIN at any time after initial provision.

6 Operational requirements

6.1 Provision and withdrawal

The SET procedures shall be provided in connection with the provision of certain telecommunication services, and shall consists of the initial registration of the PIN. This initial registration is performed by the network provider, after selection of the PIN by the served user. The PIN shall either be related to an ISDN number, or to an access or set of accesses, depending on how the telecommunication service using the PIN, is provided. The PIN shall consist of a minimum of 4 alphanumeric characters. The maximum number of characters is a network option, but shall not exceed 12 alphanumeric characters.

Withdrawal of the SET procedures is outside the scope of the present document.

As a network option the served user shall be notified when one or more attempts (but less than the blocking limit N whereby all procedures using the PIN are blocked) have been made to use an invalid PIN, either during the operation of a telecommunication service using the PIN, or during the PIN registration procedure. The blocking limit N whereby all procedures using the PIN are blocked, is also a network option.

The network options are summarized in table 1.

Table 1: Network options for the SET procedures

Network option	Value
Notification of possible fraudulent use	no yes
Maximum number of PIN characters	4 to 12
Blocking limit N	≥ 3

6.2 Requirements on the originating network side

Not applicable.

6.3 Requirements on the destination network side

Not applicable.

7 Coding requirements

7.1 Coding of the Facility information element components

Table 2 shows the definitions of the operations and errors required for the SET procedures using ASN.1 as specified in CCITT Recommendation X.208 [3] and using the OPERATION and ERROR macro as defined in figure 4 of CCITT Recommendation X.219 [4].

The formal definition of the component types to encode these operations and errors is provided in clause D.1 of EN 300 196-1 [1].

The inclusion of components in Facility information elements is defined in subclause 11.2.2.1 of EN 300 196-1 [1].

All components (invoke, return result, return error and reject) shall be included within a Facility information element. This Facility information element may be included in any appropriate message as specified in subclause 11.2.2.1 of EN 300 196-1 [1], unless a more restrictive specification is given in clause 9.

Table 2: Definition of operations and errors for the SET procedures

```
Pin-Set-Operations-and-Errors {ccitt identified-organization etsi(0) 1002 operations-and-errors(1)}

DEFINITIONS EXPLICIT TAGS ::=

BEGIN

EXPORTS
        ModifyPin,
        Pin,
        InvalidPin,
        PinNotProvided,
        InvalidNewPin,
        ChangeOfPinRequired,
        PrimitivePin,
        NewPinIsOldPin,
        UserControlBlocked
;

IMPORTS
        OPERATION, ERROR
        FROM Remote-Operation-Notation
            {joint-iso-ccitt remote-operations(4) notation(0)}

        PartyNumber
        FROM Addressing-Data-Elements
            {ccitt identified-organization etsi(0) 196 addressing-data-elements(6)}

        invalidServedUserNr
        FROM General-Errors
            {ccitt identified-organization etsi(0) 196 general-errors(2)}
;

ModifyPin               ::= OPERATION
                                ARGUMENT    ModifyPinArgument
                                RESULT
                                ERRORS     {InvalidPin,
                                            PinNotProvided,
                                            InvalidNewPin,
                                            invalidServedUserNr,
                                            PrimitivePin,
                                            NewPinIsOldPin,
                                            UserControlBlocked}

PossibleFraudulentUse   ::= OPERATION
```

Table 2 (concluded): Definition of operations and errors for the SET procedures

```
ModifyPinArgument       ::= SEQUENCE {
                                oldPin          Pin,
                                newPin          Pin,
                                servedUserNr    PartyNumber}

Pin                     ::= IA5String (SIZE(4..12)) (FROM ("0"|"1"|"2"|"3"|"4"|"5"|"6"|"7"|"8"|"9"
                                                          |"A"|"B"|"C"|"D"|"E"|"F"|"G"|"H"|"I"|"J"
                                                          |"K"|"L"|"M"|"N"|"O"|"P"|"Q"|"R"|"S"|"T"
                                                          |"U"|"V"|"W"|"X"|"Y"|"Z"
                                                          |"a"|"b"|"c"|"d"|"e"|"f"|"g"|"h"|"i"|"j"
                                                          |"k"|"l"|"m"|"n"|"o"|"p"|"q"|"r"|"s"|"t"
                                                          |"u"|"v"|"w"|"x"|"y"|"z"))

InvalidPin              ::= ERROR
PinNotProvided          ::= ERROR
InvalidNewPin           ::= ERROR
UserControlBlocked      ::= ERROR
ChangeOfPinRequired     ::= ERROR
PrimitivePin            ::= ERROR
NewPinIsOldPin          ::= ERROR

pINOID OBJECT IDENTIFIER ::= {ccitt identified-organization etsi(0) 1002 operations-and-errors(1)}

modifyPin               ModifyPin               ::= globalValue {pINOID  1}
possibleFraudulentUse   PossibleFraudulentUse   ::= globalValue {pINOID  2}
invalidPin              InvalidPin              ::= globalValue {pINOID 10}
pinNotProvided          PinNotProvided          ::= globalValue {pINOID 11}
invalidNewPin           InvalidNewPin           ::= globalValue {pINOID 12}
userControlBlocked      UserControlBlocked      ::= globalValue {pINOID 13}
changeOfPinRequired     ChangeOfPinRequired     ::= globalValue {pINOID 14}
primitivePin            PrimitivePin            ::= globalValue {pINOID 15}
newPinIsOldPin          NewPinIsOldPin          ::= globalValue {pINOID 16}

END -- of Pin-Function-Operations-and-Errors
```

7.2 Coding of the information elements

Not applicable.

8 State definitions

The following states are defined for the PIN registration procedure, associated with a specific request at the served user's access. The states only refer to the state of the request:

Table 3: States for the PIN registration procedure

User states	
Idle	This is the state as defined in subclause 10.2.6 of EN 300 196-1 [1]
Registrate Request	The user has requested the PIN registration
Network states	
Idle	This is the state as defined in subclause 10.2.6 of EN 300 196-1 [1]
Registrate Request	The network has received a PIN registration request

9 Signalling procedures at the coincident S and T reference point

9.1 Activation

Not applicable.

9.2 Deactivation

Not applicable.

9.3 Registration

The registration procedure shall be used by the served user to modify his/her PIN.

9.3.1 Normal operation

To modify his/her PIN after initial registration, the served user shall:

- send a ModifyPin invoke component to the network using the procedure described in subclause 8.3.2.2 of EN 300 196-1 [1];
- start timer T-REGISTRATE; and
- enter the Registrate Request state.

The served user shall include the following information in this invoke component:

- in the oldPin parameter, the PIN that is provided to the served user before this registration procedure is invoked;
- in the newPin parameter, the new PIN to be registered;

NOTE: The served user is actually required to input the new PIN twice. It will be a terminal function to verify that both inputs are identical.

- in the servedUserNr parameter, the ISDN number for which the registration applies.

On receipt of the ModifyPin invoke component, the network shall:

- enter the Registrate Request state; and
- for the ISDN number identified in the servedUserNr parameter, replace the currently registered PIN with the PIN identified in the newPin parameter.

If the registration is successfully performed, the network shall:

- send a ModifyPin return result component to the served user, using the procedure described in subclause 8.3.2.2 of EN 300 196-1 [1]; and
- enter the Idle state.

The served user, on receiving such a ModifyPin return result component, shall stop timer T-REGISTRATE and enter the Idle state.

9.3.2 Exceptional procedures

If the network is unable to perform the requested registration, the network shall send a ModifyPin return error component to the served user using the procedure in subclause 8.3.2.2 of EN 300 196-1 [1], and shall return to the Idle state. One of the following error values shall be indicated in the return error component (errors are listed in the order in which they shall be checked for):

- "invalidServedUserNr", if the ISDN number provided to identify the served user is not a valid number;
- "PinNotProvided", if no telecommunication service using a PIN is subscribed by the ISDN number identified in the servedUserNr parameter;
- "UserControlBlocked", if the registration request cannot be accepted due to the fact that the served user has exceeded the number of times (blocking limit N) that an invalid PIN can be used.

NOTE 1: The value of N is a network option.

- "InvalidPin", if the PIN indicated in the oldPin parameter doesn't match the currently registered PIN for the ISDN number identified in the servedUserNr parameter;
- "InvalidNewPin", if the PIN indicated in the newPin parameter has a wrong format i.e. wrong length or contains non-alphanumeric characters;
- "PrimitivePin", if the PIN indicated in the newPin parameter is a primitive PIN;

NOTE 2: The definition of primitive PINs is a network option.

- "NewPinIsOldPin", if the PIN indicated in the newPin parameter is identical to the currently registered PIN.

On receiving such a ModifyPin return error component, the served user shall stop timer T-REGISTRATE and return to the Idle state.

On expiration of timer T-REGISTRATE and the served user not having received any response to the ModifyPin invoke component, the served user shall enter the Idle state and shall consider that the attempt to modify the PIN has failed.

On receiving a reject component, the served user shall stop timer T-REGISTRATE, and shall return to the same state as before the ModifyPin invoke component was sent.

If the network receives a reject component from the served user, it need not correlate it to the procedure in this subclause.

If an entity receives a DL-RELEASE-INDICATION primitive in the Registrate Request state, then the entity shall abort the registration without informing the other entity, and enter the Idle state.

If an entity receives a DL-ESTABLISH-INDICATION primitive in the Registrate Request state, then the entity shall ignore the indication and remain in the current state.

9.4 Erasure

The registration procedure automatically erases the currently provided PIN. No additional protocol procedures are required.

9.5 Interrogation

Not applicable

9.6 Invocation and operation

Invocation of the SET procedures shall consist of using the registered PIN in association with certain telecommunication services, requiring this security tool.

9.6.1 Normal operation

The procedures related to the use of a PIN in association with telecommunication services shall be described in the appropriate telecommunication services.

9.6.2 Exceptional procedures

Related to the use of a PIN, the following error values shall be used by the telecommunication services using the SET procedures:

- "ChangeOfPinRequired", if the indicated PIN by the served user of the telecommunication service is valid, but has expired;

NOTE 1: The served user may be requested to change the PIN periodically. This is an administrative matter between the network provider and the served user. When the registered PIN expires, it is marked as such by the network provider, using an Operation And Maintenance (OAM) procedure.

- "InvalidPin", if the PIN indicated by the served user of the telecommunication service doesn't match the currently registered PIN for that served user;

- "UserControlBlocked", if the telecommunication service related request cannot be accepted due to the fact that the served user has exceeded the number of times (blocking limit N) that an invalid PIN can be used.

NOTE 2: The value of N is a network option.

9.7 Notification of possible fraudulent use

If the value of the network option "Notification of possible fraudulent use" is "yes", then the network shall send to the served user a PossibleFraudulentUse invoke component using the procedure for status notification described in subclause 10.2.5 of EN 300 196-1 [1], when one of the following conditions exist:

- one or more attempts (but less than the blocking limit N whereby all procedures using a PIN are blocked) have been made to use an invalid PIN; or

- the network option applies to automatically reinitialize the blocked SET procedures after a predefined time period, and the served user has not yet received a notification of possible fraudulent use while use of the PIN was not blocked.

This notification shall be sent when either the served user performs a PIN registration with the valid, registered PIN, or when the served user performs a procedure for a telecommunication service, protected by the SET procedures, with the valid, registered PIN.

When the Multiple Subscriber Number (MSN) supplementary service is provided to the served user, the Called party number information element shall be included and shall indicate the multiple subscriber number of the served user.

10 Procedures for interworking with private ISDNs

The SET procedures shall be provided to the whole private ISDN.

For registration at the T reference point, the procedures in subclause 9.3 of the present document shall apply except that the request shall always be applicable to the whole private ISDN access. A servedUserNr parameter in the ModifyPin invoke component shall always be ignored.

For notification of possible fraudulent use at the T reference point, the procedures in subclause 9.7 shall apply. The Called party number information element shall not be included.

11 Interaction with other networks

Not applicable.

12 Interaction with other supplementary services

Not applicable.

13 Parameter values (timers)

Table 4 shows the timer used for the PIN registration procedure.

Table 4: Timer for the PIN registration procedure

Timer	Timeout value	Cause for start	Normal stop	At expiry
T-REGISTRATE	4 seconds	Registrate invoke sent	Registrate return result received	return to Idle state

14 Dynamic description (SDL diagrams)

The SDL diagrams are specified in figures 1 to 2 according to ITU-T Recommendation Z.100 [5]. These SDL diagrams show the interaction between internal user or network events and the resulting protocol messages.

SDL input and output symbols with direction entering and leaving to the left indicate internal events.

SDL input and output symbols with direction entering or leaving to the right indicate a protocol message exchange.

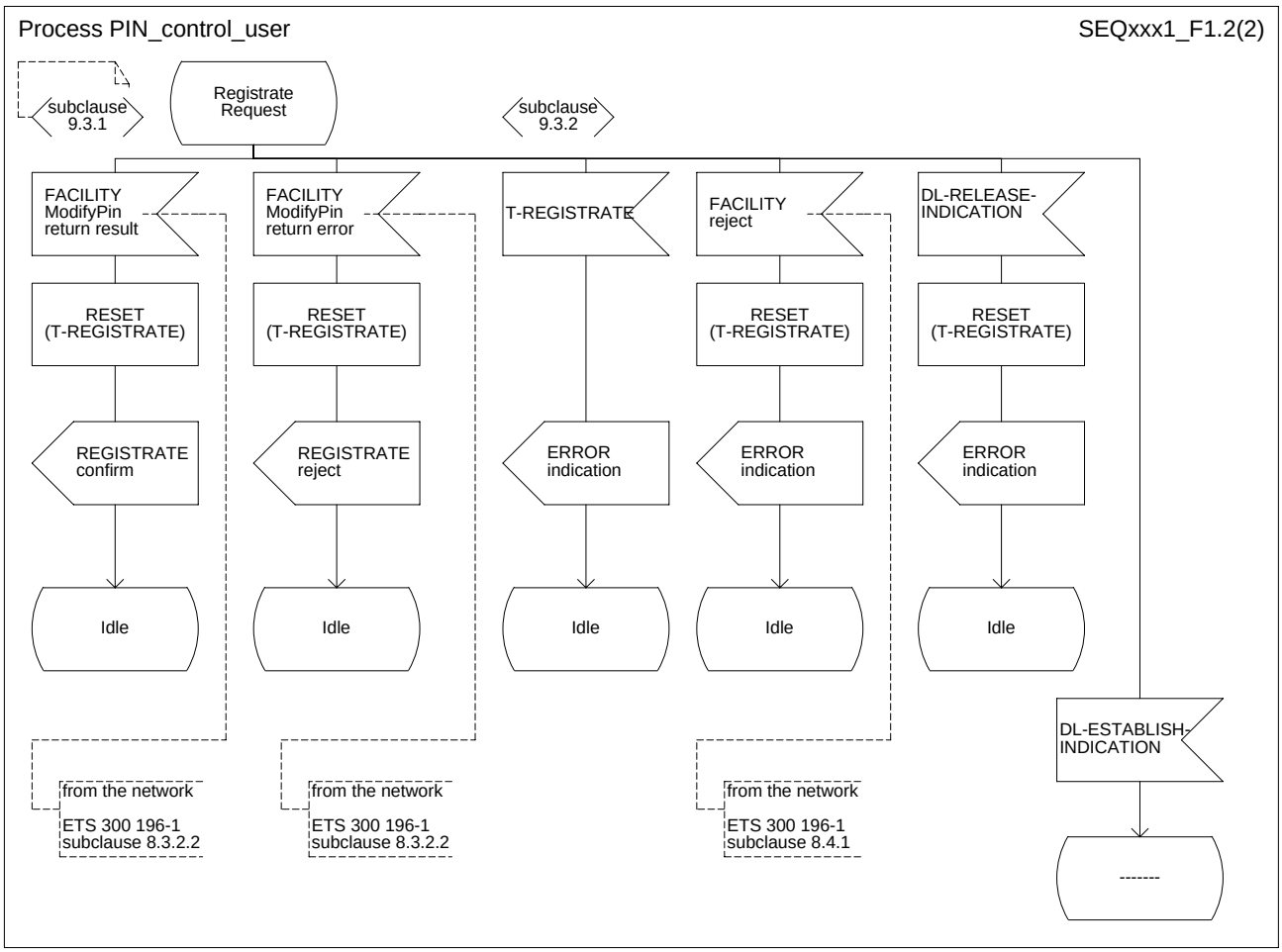

Figure 1 (sheet 1 of 2): SET management procedures - user side

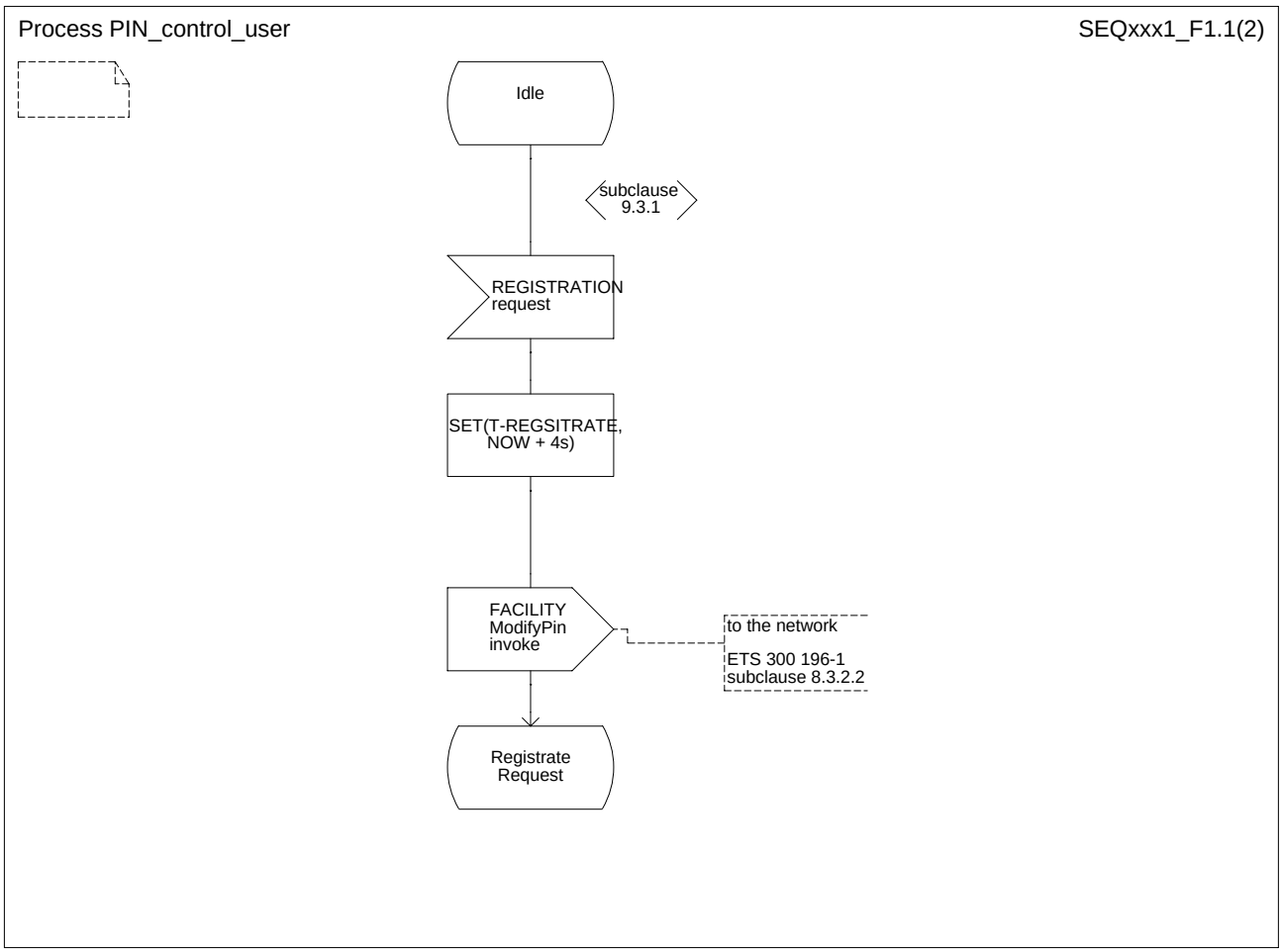

Figure 1 (sheet 2 of 2): SET management procedures - user side

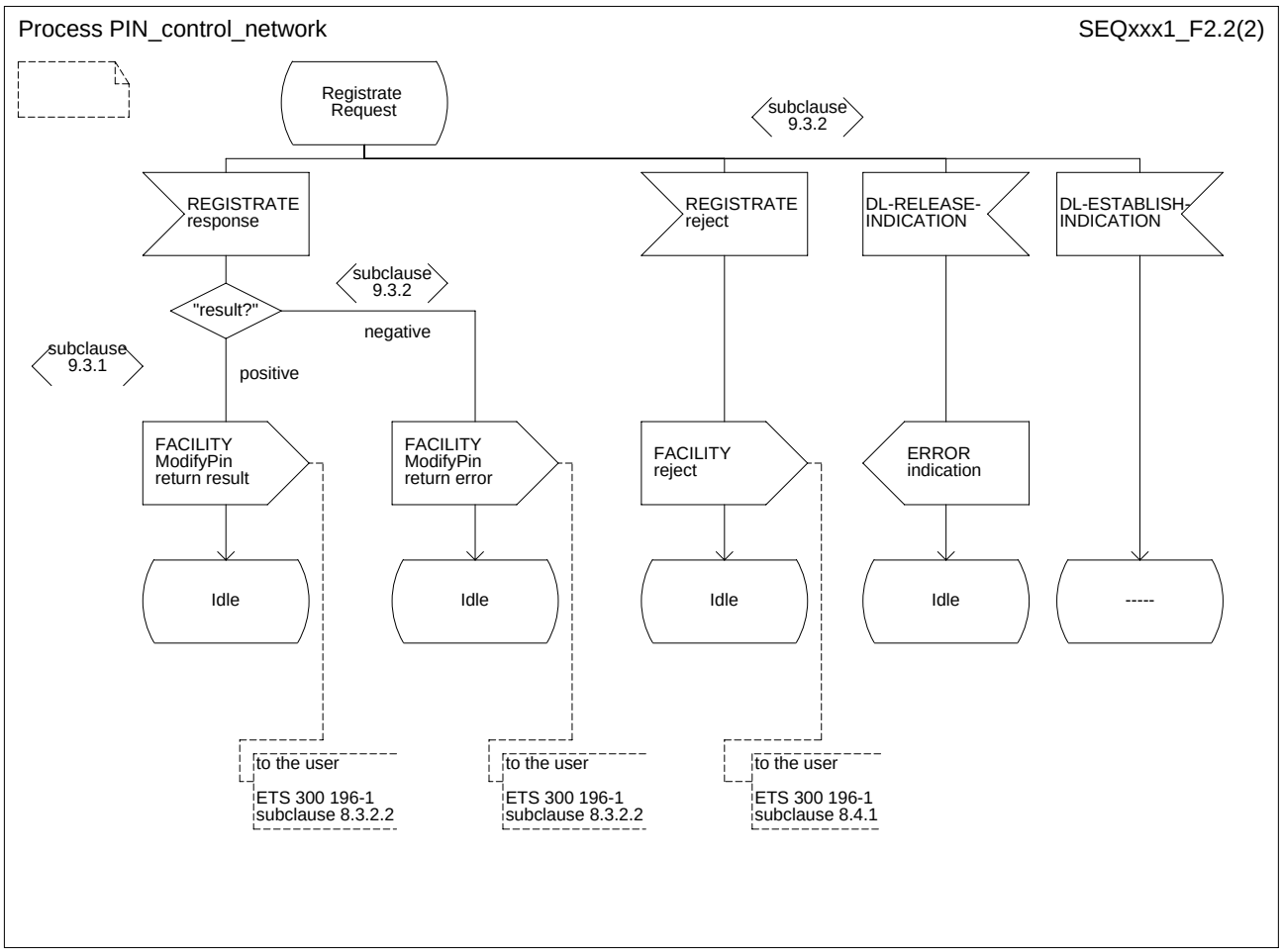

Figure 2 (sheet 1 of 2): SET management procedures - network side

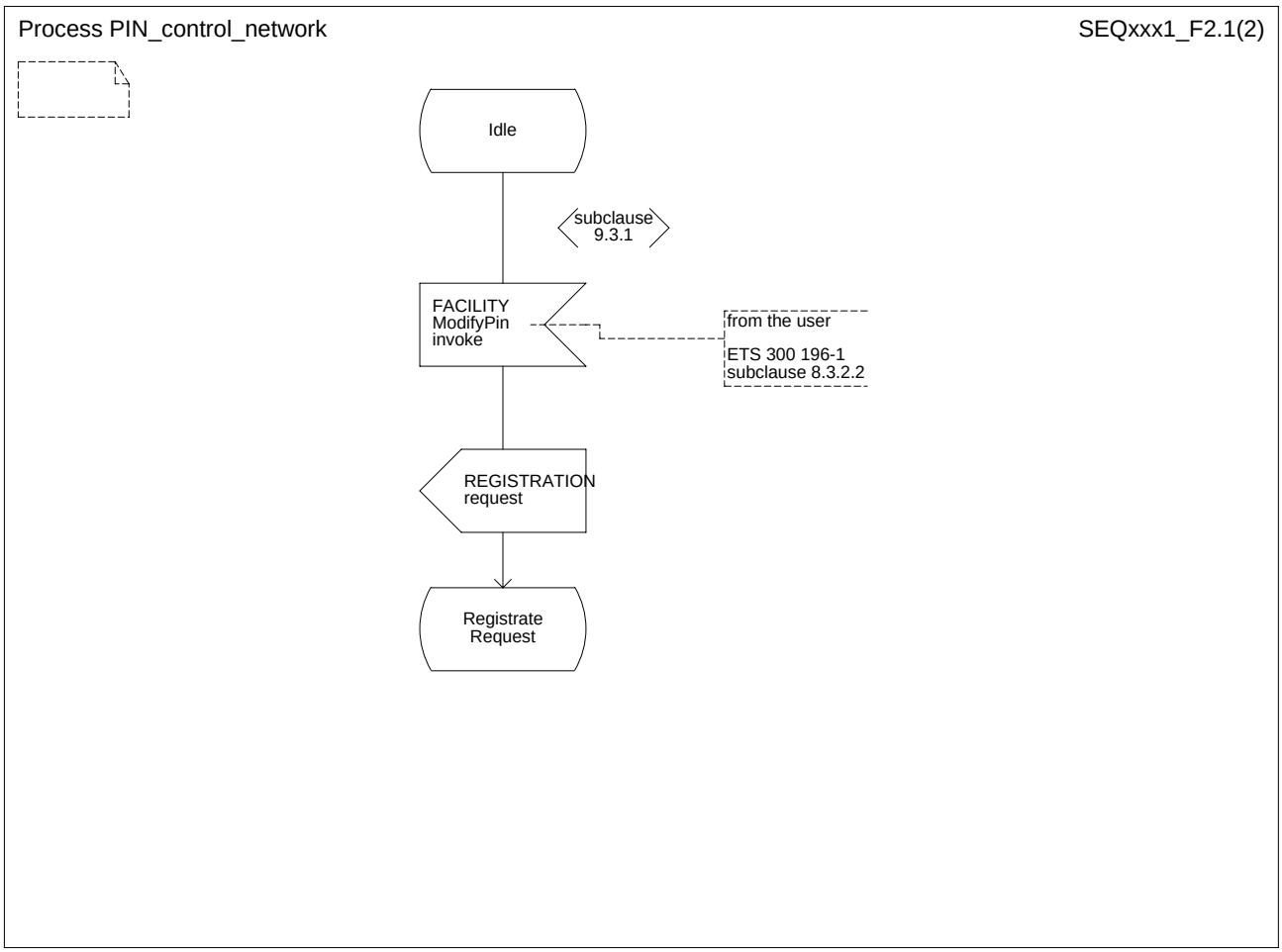

Figure 2 (sheet 2 of 2): SET management procedures - network side

Annex A (informative): Signalling flows

This annex contains the signalling flows for the following SET procedures:

Figure A.1: PIN registration by the served user

The following symbols are used in figure A.1:

DCR	Dummy Call Reference
FIE	Facility Information Element
Inv	Invoke component
Rr	Return result component

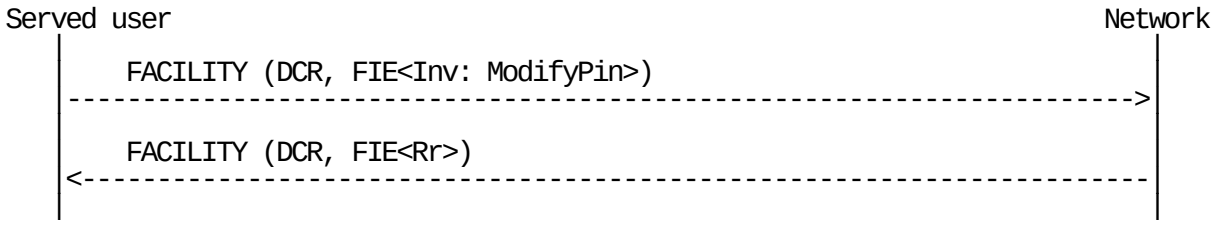

Figure A.1: PIN registration procedure

Annex B (informative): Assignment of object identifier values

The following object identifier values are assigned in the present document:

```
{ccitt identified-organization etsi(0) 1002 operations-and-errors(1)}
{ccitt identified-organization etsi(0) 1002 operations-and-errors(1)  1}
{ccitt identified-organization etsi(0) 1002 operations-and-errors(1)  2}
{ccitt identified-organization etsi(0) 1002 operations-and-errors(1) 10}
{ccitt identified-organization etsi(0) 1002 operations-and-errors(1) 11}
{ccitt identified-organization etsi(0) 1002 operations-and-errors(1) 12}
{ccitt identified-organization etsi(0) 1002 operations-and-errors(1) 13}
{ccitt identified-organization etsi(0) 1002 operations-and-errors(1) 14}
{ccitt identified-organization etsi(0) 1002 operations-and-errors(1) 15}
{ccitt identified-organization etsi(0) 1002 operations-and-errors(1) 16}
```

History

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