Standard ECMA-243
2nd Edition - September 1997

ECMA

Standardizing Information and Communication Systems

Private Integrated Services Network (PISN) - Cordless Terminal Mobility (CTM) - Inter-Exchange Signalling Protocol - Cordless Terminal Authentication Supplementary Services

Phone: +41 22 849.60.00 - **Fax:** +41 22 849.60.01 - **URL:** http://www.ecma.ch - **Internet:** helpdesk@ecma.ch

Standard ECMA-243
2nd Edition - September 1997

ECMA

Standardizing Information and Communication Systems

Private Integrated Services Network (PISN) - Cordless Terminal Mobility (CTM) - Inter-Exchange Signalling Protocol - Cordless Terminal Authentication Supplementary Services

(QSIG-CTAU)

Phone: +41 22 849.60.00 - **Fax:** +41 22 849.60.01 - **URL:** http://www.ecma.ch - **Internet:** helpdesk@ecma.ch

IW Ecma-243.doc 02-09-97 16,00

Brief History

This Standard is one of a series of ECMA Standards defining services and signalling protocols applicable to Private Integrated Services Networks (PISNs). The series uses ISDN concepts as developed by ITU-T and conforms to the framework of International Standards for Open Systems Interconnection as defined by ISO/IEC. It has been produced under ETSI work item DE/ECMA-00116.

This particular Standard specifies the signalling protocol for use at the Q reference point in support of the Cordless Terminal Authentication supplementary services. The protocol defined in this Standard forms part of the PSS1 protocol (informally known as QSIG).

This Standard is based upon the practical experience of ECMA member companies and the results of their active and continuous participation in the work of ISO/IEC JTC1, ITU-T, ETSI and other international and national standardization bodies. It represents a pragmatic and widely based consensus.

Compared to the 1st Edition of Standard ECMA-243 (published by ECMA in June 1996), various changes have been made in order to achieve alignment with I-ETS 300 809 (which is based on the 1st Edition of ECMA-243 but modified during Public Enquiry).

Adopted as 2nd Edition of Standard ECMA-243 by the General Assembly in September 1997.

Table of contents

.

1 Scope

This Standard specifies the signalling protocol for the support of the Authentication supplementary services (SS-CTAT and SS-CTAN) at the Q reference point between Private Integrated Services Network Exchanges (PINXs) connected together within a Private Integrated Services Network (PISN).

The authentication services consist of the two following related but distinct supplementary services:

a) Authentication of a CTM user (SS-CTAT) is a supplementary service that enables a PISN, as a security measure, to validate the identity provided by the CTM user.

b) Authentication of the PISN (SS-CTAN) is a supplementary service that enables a served CTM user, as a security measure, to validate the identity of the PISN.

The mechanisms used in these services are based on the challenge and response method of authentication.

Authentication algorithms to be used by these supplementary services are outside the scope of this Standard.

Roaming outside the PISN is outside the scope of this edition of this Standard.

The Q reference point is defined in ISO/IEC 11579-1.

Service specifications are produced in three stages and according to the method specified in ETS 300 387. This Standard contains the stage 3 specification for the Q reference point and satisfies the requirements identified by the stage 1 and stage 2 specifications in I-ETS 300 768 and I-ETS 300 769.

The signalling protocol for SS-CTAT and SS-CTAN uses certain aspects of the generic procedures for the control of supplementary services specified in ECMA-165.

This Standard also specifies additional signalling protocol requirements for the support of interactions at the Q reference point between SS-CTAT/SS-CTAN and other supplementary services and ANFs.

NOTE 1

Additional interactions that have no impact on the signalling protocol at the Q reference point can be found in the relevant stage 1 specifications.

This Standard is applicable to PINXs which can interconnect to form a PISN.

2 Conformance

In order to conform to this Standard, a PINX shall satisfy the requirements identified in the Protocol Implementation Conformance Statement (PICS) proforma in annex A.

Conformance to this Standard includes conforming to those clauses that specify protocol interactions between SS-CTAT/SS-CTAN and other supplementary services and ANFs for which signalling protocols at the Q reference point are supported in accordance with the stage 3 standards concerned.

3 References (normative)

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

In the case of references to ECMA Standards that are aligned with ISO/IEC International Standards, the number of the appropriate ISO/IEC International Standard is given in brackets after the ECMA reference.

ECMA-142 Private Integrated Services Network - Circuit-mode 64 kbit/s Bearer Services - Service Description, Functional Capabilities and Information Flows (International Standard ISO/IEC 11574)

ECMA-165 Private Integrated Services Network - Generic Functional Protocol for the Support of Supplementary Services - Inter-Exchange Signalling Procedures and Protocol (International Standard ISO/IEC 11582)

ECMA-216	Private Integrated Services Network - Cordless Terminal Mobility (CTM) - Inter-Exchange Signalling Protocol - Cordless Terminal Location Registration Supplementary Service
ISO/IEC 11571	Information technology - Telecommunications and information exchange between systems - Numbering and sub-addressing in private integrated services networks
ISO/IEC 11579-1	Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Part 1: Reference configuration for PISN Exchanges (PINX)
ETS 300 387	Private Telecommunication Network (PTN); Method for the specification of basic and supplementary services (1994)
ETS 300 692	Private Integrated Services Network (PISN); Cordless Terminal Mobility (CTM); Location handling services; Functional capabilities and information flows (1995)
ITU-T Rec. I.112	Vocabulary of terms for ISDNs (1993)
ITU-T Rec. I.210	Principles of telecommunication services supported by an ISDN and the means to describe them (1993)
ITU-T Rec. Q.950	Digital Subscriber Signalling System No. 1 (DSS1) - Supplementary services protocols, structure and general principles (1993)
ITU-T Rec. Z.100	Specification and description language (1993)

4 Definitions

For the purposes of this Standard, the following definitions apply.

4.1 External definitions

This Standard uses the following terms defined in other documents:

- Application Protocol Data Unit (APDU) (ECMA-165)
- Coordination Function (ECMA-165)
- End PINX (ECMA-165)
- Home Data Base (HDB) (ECMA-216)
- Home PINX (ETS 300 692)
- Network Facility Extension (NFE) (ECMA-165)
- Originating PINX (ECMA-165)
- Private Integrated Services Network (PISN) (ISO/IEC 11579-1)
- Private Integrated Services Network Exchange (PINX) (ISO/IEC 11579-1)
- PISN Number (ISO/IEC 11571)
- Signalling (ITU-T Rec. I.112)
- Supplementary Service (ITU-T Rec. I.210)
- Supplementary Services Control Entity (ECMA-165)
- Terminating PINX (ECMA-165)
- Transit PINX (ECMA-165)
- User (ECMA-142)
- Visitor area (ECMA-216)
- Visitor PINX (ETS 300 692)

4.2 Authentication Server PINX

The PINX that provides the parameters for the authentication of a CTM user. It contains the functionality to compute the challenge to be sent to a CTM user and the expected response value from the CTM user during SS-CTAT. It also contains the functionality to compute the response value to be sent to the CTM user during SS-CTAN.

NOTE 2

The Authentication Server PINX and the Home PINX may be the same PINX.

4.3 Cordless Terminal Mobility (CTM) User

A user that requests SS-CTAN or is the target of SS-CTAT.

5 List of acronyms

ANF	Additional Network Feature
APDU	Application Protocol Data Unit
ASN.1	Abstract Syntax Notation no. 1
CT	Cordless Terminal
CTM	Cordless Terminal Mobility
HDB	Home Data Base
ISDN	Integrated Services Digital Network
NFE	Network Facility Extension
PICS	Protocol Implementation Conformance Statement
PINX	Private Integrated Services Network Exchange
PISN	Private Integrated Services Network
SDL	Specification and Description Language
SS-CTAN	Supplementary service - Authentication of a PISN
SS-CTAT	Supplementary service - Authentication of a CTM user

6 Signalling protocol for the support of SS-CTAT

6.1 SS-CTAT description

SS-CTAT is a supplementary service which enables the PISN, as a security measure, to validate the identity provided by the CTM user. This is done by sending specific information to the CTM user and awaiting a response. If the response is not the expected response, the PISN shall be informed and can take any action as appropriate.

6.2 SS-CTAT operational requirements

6.2.1 Requirements on the Visitor PINX

Generic procedures for the call-independent control (connection-oriented) of supplementary services, as specified in ECMA-165 for an Originating and Terminating PINX, shall apply.

6.2.2 Requirements on the Home PINX

Generic procedures for the call-independent control (connection-oriented) of supplementary services, as specified in ECMA-165 for an Originating and Terminating PINX, shall apply.

6.2.3 Requirements on the Authentication Server PINX

Generic procedures for the call-independent control (connection-oriented) of supplementary services, as specified in ECMA-165 for a Terminating PINX, shall apply.

6.2.4 Requirements on a Transit PINX

Generic procedures for the call-independent control (connection-oriented) of supplementary services, as specified in ECMA-165 for a Transit PINX, shall apply.

6.3 SS-CTAT coding requirements

6.3.1 Operations

The operations authCtmUser, getCtatParam, ctatParamEnq and transferAuthParam defined in the Abstract Syntax Notation number 1 (ASN.1) in table 1 shall apply to SS-CTAT.

Table 1 - Operations in support of authentication services

```
CT-Authentication-Operations
        { iso (1) identified-organization (3) icd-ecma (0012) standard (0)
        qsig-authentication(243) authentication-operations (0) }
DEFINITIONS EXPLICIT TAGS ::=
BEGIN
IMPORTS   OPERATION, ERROR FROM Remote-Operation-Notation
              { joint-iso-ccitt (2) remote-operations (4) notation (0) }
          Extension FROM Manufacturer-specific-service-extension-definition
              { iso (1) standard (0) pss1-generic-procedures (11582) msi-definition (0) }
          invalidServedUserNr FROM General-Error-List
              { ccitt (0) recommendation (0) q (17) 950 general-error-list (1) }
          PartyNumber FROM Addressing-Data-Elements
              { iso (1) standard (0) pss1-generic-procedure (11582)
              addressing-data-elements (9)};
-- The following three operations shall apply to SS-CTAT --
AuthCtmUser ::=   OPERATION -- from Home PINX to Visitor PINX--
                  ARGUMENT      AuthCtmArg
                  RESULT        AuthCtmRes
                  ERRORS        { temporarilyUnavailable, invalidServedUserNr, notAuthorized,
                                paramNotAvailable, unspecified}
GetCtatParam ::=  OPERATION -- from Visitor PINX to Home PINX --
                  ARGUMENT      CtatParamArg
                  RESULT        CtatParamRes
                  ERRORS        { invalidServedUserNr, notAuthorized,
                                paramNotAvailable, temporarilyUnavailable, unspecified}
CtatParamEnq ::=  OPERATION -- from Home PINX to Authentication Server PINX--
                  ARGUMENT      CtatParamArg
                  RESULT        CtatParamRes
                  ERRORS        { invalidServedUserNr, paramNotAvailable, unspecified}
AuthCtmArg ::=    SEQUENCE      {pisnNumber         PartyNumber,
                                calcCtatInfo        [ 1 ] IMPLICIT CalcCtatInfo OPTIONAL,
                                dummyExtension      DummyExtension OPTIONAL}
AuthCtmRes ::=    SEQUENCE      {ENUMERATED         {auth-res-correct (0),
                                                    auth-res-incorrect (1)},
                                dummyExtension      DummyExtension OPTIONAL}
```

Table 1 - Operations in support of authentication services (continued)

```
CtatParamArg ::=    SEQUENCE        {pisnNumber         PartyNumber,
                                     canCompute         CanCompute OPTIONAL,
                                     dummyExtension     DummyExtension OPTIONAL}
                -- The presence of element canCompute indicates that the Visitor PINX is able to --
                -- compute a challenge and the expected response from session key information --
CtatParamRes ::=    SEQUENCE        {ctatParamInfo      CtatParamInfo,
                                     dummyExtension     DummyExtension OPTIONAL}

-- The following two operations shall apply to SS-CTAN --
GetCtanParam ::=    OPERATION -- from Visitor PINX to Home PINX --
                    ARGUMENT        CtanParamArg
                    RESULT          CtanParamRes
                    ERRORS          { invalidServedUserNr, notAuthorized,
                                      paramNotAvailable, temporarilyUnavailable, unspecified}
CtanParamEnq ::=    OPERATION -- from Home PINX to Authentication Server PINX--
                    ARGUMENT        CtanParamArg
                    RESULT          CtanParamRes
                    ERRORS          { invalidServedUserNr, paramNotAvailable, unspecified}
CtanParamArg ::=    SEQUENCE        {pisnNumber         PartyNumber,
                                     authChallenge      AuthChallenge,
                                     authAlgorithm      AuthAlgorithm,
                                     canCompute         CanCompute OPTIONAL,
                                     dummyExtension     DummyExtension OPTIONAL}
                -- The presence of element canCompute indicates that the Visitor PINX is able to --
                -- compute the response from session key information --
CtanParamRes ::=    SEQUENCE        { ctanParamInfo     CtanParamInfo,
                                     dummyExtension     DummyExtension OPTIONAL}

-- The following unconfirmed operation shall apply when interaction between SS-CTAT and SS-CTLR
TransferAuthParam  ::=OPERATION -- from previous Visitor PINX to Visitor PINX --
                       ARGUMENT SEQUENCE    {CtatParamInfo,
                                             DummyExtension OPTIONAL}
CtatParamInfo ::=   SEQUENCE {authAlgorithm      AuthAlgorithm,
                              CHOICE {
                                     authSessionKeyInfo     [ 1 ] IMPLICIT AuthSessionKeyInfo,
                                     calcCtatInfo           [ 2 ] IMPLICIT CalcCtatInfo} }
CtanParamInfo ::=   CHOICE          {authSessionKeyInfo     [ 1 ] IMPLICIT AuthSessionKeyInfo,
                                     calcCtanInfo           [ 2 ] IMPLICIT CalcCtanInfo}
AuthSessionKeyInfo ::= SEQUENCE     { authSessionKey        AuthSessionKey,
                                      calculationParam      CalculationParam}
CalcCtatInfo ::=    SEQUENCE SIZE(1..5) OF CalcCtatInfoUnit
CalcCtatInfoUnit ::=SEQUENCE        {authChallenge          AuthChallenge,
                                     authResponse           AuthResponse,
                                     derivedCipherKey       [1] IMPLICIT DerivedCipherKey OPTIONAL,
                                     calculationParam       [2] IMPLICIT CalculationParam OPTIONAL}
                                     -- included if required by the authentication algorithm in use --
```

Table 1 - Operations in support of authentication services (concluded)

```
CalcCtanInfo ::=      SEQUENCE      {authResponse       AuthResponse,
                                    calculationParam    CalculationParam OPTIONAL}
                                    -- included if required by the authentication algorithm in use --
DummyExtension ::= CHOICE           {extension          [3] IMPLICIT Extension,
                                    sequOfExtn          [4] IMPLICIT SEQUENCE OF Extension}
AuthAlgorithm ::=     INTEGER {     -- type of authentication algorithm --
                                    ct2 (0)
                                    dect (1)
                                    gsm (2)
                                    us-ct2 (3)
                                    us-dect (4)
                                    us-gsm (5)
                                    } (0..255)   -- Other name values may be defined in the future --
AuthChallenge ::=     OCTET STRING (SIZE(1-8))      -- Randomly generated parameter --
AuthResponse ::=      OCTET STRING (SIZE(1-4))      -- CTAT: Expected response value --
                                                    -- CTAN: Response value from network --
AuthSessionKey ::=OCTET STRING (SIZE(1-16))         -- Authentication session key--
CalculationParam ::= OCTET STRING (SIZE(1-8))       -- Parameter used when calculating --
                                                    -- the authentication session key from --
                                                    -- the real authentication key. It may be --
                                                    -- transferred to the CTM user during --
                                                    -- both CTAT and CTAN. --
CanCompute ::=        NULL                          -- indicates capability of computing --
                                                    -- challenge and/or response value --
DerivedCipherKey ::= OCTET STRING (SIZE(1-8))       -- derived cipher key may be computed --
                                                    -- when computing challenge and --
                                                    -- expected response values--
authCtmUser           AuthCtmUser           ::=     72
getCtatParam          GetCtatParam          ::=     73
ctatParamEnq          CtatParamEnq          ::=     74
getCtanParam          GetCtanParam          ::=     75
ctanParamEnq          CtanParamEnq          ::=     76
transferAuthParam     TransferAuthParam     ::=     77
notAuthorized         ERROR                 ::=     1007
paramNotAvailable     ERROR                 ::=     1017
temporarilyUnavailable ERROR                ::=     1000
unspecified           Unspecified           ::=     1008
Unspecified ::=       ERROR       PARAMETER Extension
END             -- of CT-Authentication-Operations
```

6.3.2 Information elements

6.3.2.1 Facility information element

The operations defined in 6.3.1 shall be coded in the Facility information element in accordance with ECMA-165.

When conveying the invoke APDU of operations defined in 6.3.1, the destinationEntity data element of the NFE shall contain value endPINX.

When conveying the invoke APDU of operations defined in 6.3.1, the interpretation APDU shall either be omitted or be included with the value rejectAnyUnrecognisedInvokePdu.

6.3.2.2 Other information elements

Any other information elements (e.g. Calling party number, Called party number) shall be coded in accordance with ECMA-165.

6.3.3 Messages

The Facility information element shall be conveyed in the messages as specified in clause 10 of ECMA-165.

6.4 SS-CTAT state definitions

6.4.1 States at the Home PINX for initiation of SS-CTAT

The procedures for the Home PINX for initiation of SS-CTAT are written in terms of the following conceptual states existing within the SS-CTAT Supplementary Service Control entity in that PINX in association with a particular request for authentication of a CTM user.

6.4.1.1 State CtatHomeInitIdle

Initiation of SS-CTAT in the Home PINX is not in progress.

6.4.1.2 State CtatHomeInitiating

An authCtmUser invoke APDU has been sent to the Visitor PINX.

6.4.2 States at the Home PINX for requesting authentication parameters

The procedures for the Home PINX for requesting authentication parameters are written in terms of the following conceptual states existing within the SS-CTAT Supplementary Service Control entity in that PINX in association with a particular request for authentication of a CTM user.

6.4.2.1 State CtatHomeRequestIdle

Ready for receipt of a getCtatParam invoke APDU from the Visitor PINX.

6.4.2.2 State CtatHomeRequesting

A getCtatParam invoke APDU has been received from the Visitor PINX.

6.4.3 States at the Home PINX when fetching authentication parameters

The procedures for the Home PINX when fetching authentication parameters are written in terms of the following conceptual states existing within the SS-CTAT Supplementary Service Control entity in that PINX in association with a particular request for authentication of a CTM user.

6.4.3.1 State CtatHomeFetchIdle

Fetching of authentication parameters from the Authentication Server PINX during SS-CTAT is not in progress.

6.4.3.2 State CtatHomeFetching

A ctatParamEnq invoke APDU has been sent to the Authentication Server PINX.

6.4.4 States at the Visitor PINX for execution of SS-CTAT

The procedures for the Visitor PINX for execution of SS-CTAT are written in terms of the following conceptual states existing within the SS-CTAT Supplementary Service Control entity in that PINX in association with a particular request for authentication of a CTM user.

6.4.4.1 State CtatVisitExecIdle

Execution of SS-CTAT is not in progress.

6.4.4.2 State CtatVisitExecuting

An authCtmUser invoke APDU has been received from the Home PINX and execution of SS-CTAT is in progress.

6.4.5 States at the Visitor PINX for requesting authentication parameters

The procedures for the Visitor PINX for requesting authentication parameters are written in terms of the following conceptual states existing within the SS-CTAT Supplementary Service Control entity in that PINX in association with a particular request for authentication of a CTM user.

6.4.5.1 State CtatVisitRequestIdle

Request for authentication parameters from the Home PINX during SS-CTAT is not in progress.

6.4.5.2 State CtatVisitRequesting

A getCtatParam invoke APDU has been sent to the Home PINX.

6.4.6 States at the Authentication Server PINX

The procedures for the Authentication Server PINX are written in terms of the following conceptual states existing within the SS-CTAT Supplementary Service Control entity in that PINX in association with a particular request for authentication of a CTM user.

6.4.6.1 State CtatAuthenticationIdle

Ready for receipt of a ctatParamEnq invoke APDU from the Home PINX.

6.5 SS-CTAT signalling procedures

Examples of message sequences are shown in annex B.

6.5.1 Actions at the Home PINX for initiation of SS-CTAT

The SDL representation of procedures at the Home PINX for initiation of SS-CTAT is shown in C.1 of annex C.

6.5.1.1 Normal procedures

On determining that the SS-CTAT is to be invoked without providing challenge and response values to the Visitor PINX, the Home PINX shall send an authCtmUser invoke APDU to the Visitor PINX where element calcCtatInfo is omitted.

On determining that the SS-CTAT is to be invoked with challenge and response values provided to the Visitor PINX, the Home PINX shall use the procedures of 6.5.3 for enquiry to the Authentication Server PINX to fetch challenge and response values. On receipt of challenge and response values from the Authentication Server PINX, the Home PINX shall send an authCtmUser invoke APDU to the Visitor PINX containing the element calcCtatInfo.

The authCtmUser invoke APDU shall be sent to the Visitor PINX using the call reference of a call-independent signalling connection. The call-independent signalling connection shall be established (or used, if an appropriate connection is already available) in accordance with the procedures specified in 7.3 of ECMA-165. The Home PINX shall enter state CtatHomeInitiating and start timer T1.

On receipt of the authCtmUser return result APDU, the Home PINX shall stop timer T1 and enter state CtatHomeInitIdle.

NOTE 3

Confirmation of the authentication of the CTM user should be indicated to the initiating entity.

The Home PINX is responsible for clearing the call-independent signalling connection towards the Visitor PINX. This may occur on receipt of a return result APDU. Alternatively, the signalling connection may be retained for other applications, if appropriate.

6.5.1.2 Exceptional procedures

On receipt of an authCtmUser return error or reject APDU from the Visitor PINX, the Home PINX shall stop timer T1 and enter state CtatHomeInitIdle.

If timer T1 expires (i.e. the authCtmUser invoke APDU is not answered by the Visitor PINX), the Home PINX shall enter state CtatHomeInitIdle.

NOTE 4

Failure of the authentication of the CTM user should be indicated to the initiating entity.

The Home PINX is responsible for clearing the call-independent signalling connection towards the Visitor PINX. This may occur on receipt of a return error or reject APDU or on expiry of timer T1. Alternatively, the signalling connection may be retained for other applications, if appropriate.

6.5.2 Actions at the Home PINX for requesting authentication parameters

The SDL representation of procedures at the Home PINX for requesting authentication parameters is shown in C.2 of annex C.

6.5.2.1 Normal procedures

On receipt of a getCtatParam invoke APDU using the call reference of a call-independent signalling connection (as specified in 7.3 of ECMA-165), the Home PINX shall check that the received PISN number of the CTM user is valid and that the CTM user is authorised for SS-CTAT. The Home PINX shall then enter state CtatHomeRequesting and initiate fetching of the authentication parameters from the Authentication Server PINX using the procedures of 6.5.3. When the authentication parameters are available, the Home PINX shall answer the getCtatParam invoke APDU with a return result APDU containing the authentication parameters received from the Authentication Server PINX. The Home PINX shall enter state CtatHomeRequestIdle.

6.5.2.2 Exceptional procedures

If the received PISN number is not valid, the Home PINX shall answer the getCtatParam invoke APDU with a return error APDU containing the error invalidServedUserNr and remain in state CtatHomeRequestIdle.

If the CTM user is not authorised for SS-CTAT, the Home PINX shall answer the getCtatParam invoke APDU with a return error APDU containing the error notAuthorized and remain in state CtatHomeRequestIdle.

If authentication parameters are not received for any reason during the procedures of 6.5.3, the Home PINX shall answer the getCtatParam invoke APDU with a return error APDU and enter state CtatHomeRequestIdle. In case of time out error value temporarilyUnavailable shall be included. In all other cases, error paramNotAvailable shall be included.

6.5.3 Actions at the Home PINX when fetching authentication parameters

The SDL representation of procedures at the Home PINX when fetching authentication parameters from the Authentication Server PINX is shown in C.3 of annex C.

When a Home PINX also provides Authentication Server PINX functionality, the joint requirements of 6.5.3 (for a Home PINX) and 6.5.7 (for an Authentication Server PINX) shall apply, with the exception that any communication between the Home PINX functionality and the Authentication Server PINX functionality will be an intra-PINX matter. The messages specified for sending from the Home PINX towards the Authentication Server PINX or vice versa will not appear on any inter-PINX link.

6.5.3.1 Normal procedures

On receipt of a request for fetching authentication parameters, the Home PINX shall send a ctatParamEnq invoke APDU to the Authentication Server PINX using the call reference of a call-independent signalling connection. Element canCompute shall be omitted, unless the Visitor PINX has indicated (by element canCompute in the argument of a getCtatParam invoke APDU) that it is able to compute its own challenge and response. The call-independent signalling connection shall be established (or used, if an appropriate connection is already available) in accordance with the procedures specified in 7.3 of ECMA-165. The Home PINX shall enter state CtatHomeFetching and start timer T2.

On receipt of the ctatParamEnq return result APDU, the Home PINX shall stop timer T2 and enter state CtatHomeFetchIdle.

The Home PINX is responsible for clearing the call-independent signalling connection towards the Authentication Server PINX. This may occur on receipt of a return result APDU. Alternatively, the signalling connection may be retained for other applications, if appropriate.

6.5.3.2 Exceptional procedures

On receipt of a ctatParamEnq return error or reject APDU from the Authentication Server PINX, the Home PINX shall stop timer T2 and enter state CtatHomeFetchIdle.

If timer T2 expires (i.e. the ctatParamEnq invoke APDU is not answered by the Authentication Server PINX), the Home PINX shall enter state CtatHomeFetchIdle.

The Home PINX is responsible for clearing the call-independent signalling connection towards the Authentication Server PINX. This may occur on receipt of a return error or reject APDU or on expiry of timer T2. Alternatively, the signalling connection may be retained for other applications, if appropriate.

6.5.4 Actions at the Visitor PINX for local initiation of SS-CTAT

The SDL representation of procedures at the Visitor PINX for requesting authentication parameters from the Home PINX is shown in C.5 of annex C.

6.5.4.1 Normal procedures

On determining that the SS-CTAT is to be invoked and when the authentication parameters are not available in the Visitor PINX for this CTM user, the Visitor PINX shall use the procedures of 6.5.6 to make an enquiry to the Home PINX in order to get the authentication parameters. If the Visitor PINX is capable of calculating challenge and response values, the element canCompute shall be included. On receipt of the authentication parameters from the Home PINX, the SS-CTAT shall be executed.

6.5.4.2 Exceptional procedures

If the authentication parameters were not received during the procedures of 6.5.6, SS-CTAT will not be executed.

6.5.5 Actions at the Visitor PINX for execution of SS-CTAT

The SDL representation of procedures at the Visitor PINX for execution of SS-CTAT is shown in C.4 of annex C.

6.5.5.1 Normal procedures

On receipt of an authCtmUser invoke APDU using the call reference of a call-independent signalling connection (as specified in 7.3 of ECMA-165) and when either element calcCtatInfo is included or authentication parameters for this CTM user are already available at the Visitor PINX, a request for authentication shall be sent to the CTM user and the Visitor PINX shall enter state CtatVisitExecuting.

If the element calcCtatInfo is not included in the authCtmUser invoke APDU and when the authentication parameters for this CTM user are not available at the Visitor PINX, the Visitor PINX shall enter state CtatVisitExecuting. During this state the Visitor PINX shall use the procedures of 6.5.6 to make an enquiry to the Home PINX to request the authentication parameters. If the Visitor PINX is capable of calculating challenge and response values, the element canCompute shall be included. On receipt of the authentication parameters from the Authentication Server PINX, a request for authentication shall be sent to the CTM user.

On receipt of the Authentication result from the CTM user, the Visitor PINX shall check the received result. If the Authentication result from CTM user is correct, the Visitor PINX shall answer the authCtmUser invoke APDU with a return result APDU indicating CT authentication result correct. If the Authentication result is incorrect, the Visitor PINX shall answer the authCtmUser invoke APDU with a return result APDU indicating CT authentication result incorrect. The Visitor PINX shall enter state CtatVisitExecIdle.

6.5.5.2 Exceptional procedures

If authentication parameters are not received for any reason during the procedures of 6.5.6, the Visitor PINX shall answer the authCtmUser invoke APDU with a return error APDU and enter state CtatVisitExecIdle.

If the authentication request is not answered by the CTM user, the Visitor PINX shall answer the authCtmUser invoke APDU with a return error APDU containing the error temporarilyUnavailable and enter state CtatVisitExecIdle. The error value shall be included in accordance with clause 6.5.2.2.

6.5.6 Actions at the Visitor PINX for requesting authentication parameters

The SDL representation of procedures at the Visitor PINX for requesting authentication parameters from the Home PINX is shown in C.5 of annex C.

6.5.6.1 Normal procedures

In order to make an enquiry to the Home PINX to request the authentication parameters for a CTM user, the Visitor PINX shall send a getCtatParam invoke APDU to the Home PINX using the call reference of a call-independent signalling connection. The call-independent signalling connection shall be established (or used, if an appropriate connection is already available) in accordance with the procedures specified in 7.3 of ECMA-165. The Visitor PINX shall start timer T3 and enter state CtatVisitRequesting.

On receipt of the getCtatParam return result APDU, the Visitor PINX shall stop timer T3 and enter state CtatVisitRequestIdle. If the element ctatParamInfo contains authentication session key, the Visitor PINX shall calculate the challenge and the expected response, otherwise the Visitor PINX shall use the challenge and response values as received.

NOTE 5

If several challenge/response pairs are returned in CalcCtatInfo then the Visitor PINX may store them for use in subsequent SS-CTAT executions.

The Visitor PINX is responsible for clearing the call-independent signalling connection towards the Home PINX. This may occur on receipt of a return result APDU. Alternatively, the signalling connection may be retained for other applications, if appropriate.

6.5.6.2 Exceptional procedures

On receipt of a getCtatParam return error or reject APDU from the Home PINX, the Visitor PINX shall stop timer T3 and enter state CtatVisitRequestIdle.

If timer T3 expires (i.e. the getCtatParam invoke APDU is not answered by the Home PINX), the Visitor PINX shall enter state CtatVisitRequestIdle.

The Visitor PINX is responsible for clearing the call-independent signalling connection towards the Home PINX. This may occur on receipt of a return error or reject APDU or on expiry of timer T3. Alternatively, the signalling connection may be retained for other applications, if appropriate.

6.5.7 Actions at the Authentication Server PINX

The SDL representation of procedures at the Authentication Server PINX is shown in C.6 of annex C.

6.5.7.1 Normal procedures

On receipt of a ctatParamEnq invoke APDU using the call reference of a call-independent signalling connection (as specified in 7.3 of ECMA-165), the Authentication Server PINX shall check that the received PISN number of the CTM user is valid and retrieve the authentication parameters if available. If it is required by the application or if the element canCompute is not included in the ctatParamEnq invoke APDU, the Authentication Server PINX shall use the authentication keys to compute challenge(s) and the expected response value(s), and answer the ctatParamEnq invoke APDU with a return result APDU where element ctatParamInfo contains the calculated authentication information (choice calcCtatInfo). If the element canCompute is included in the ctatParamEnq invoke APDU and if it is not required by the application to compute a challenge and the expected response value, the Authentication Server PINX shall answer the ctatParamEnq invoke APDU with a return result APDU where element ctatParamInfo contains the authentication session key (choice authSessionKeyInfo). The ctatParamEnq return result APDU shall contain the authentication algorithm in use. The Authentication Server PINX shall remain in state CtatAuthenticationIdle.

6.5.7.2 Exceptional procedures

If the received PISN number is not valid, the Authentication Server PINX shall answer the ctatParamEnq invoke APDU with a return error APDU containing the error invalidServedUserNr and remain in state CtatAuthenticationIdle.

If the authentication parameters are not available, the Authentication Server PINX shall answer the ctatParamEnq invoke APDU with a return error APDU containing the error paramNotAvailable. The Authentication Server PINX shall remain in state CtatAuthenticationIdle.

6.5.8 Actions at a Transit PINX

No special actions are required in support of authentication of a CTM user.

6.6 SS-CTAT impact of interworking with public ISDNs

Not applicable.

6.7 SS-CTAT impact of interworking with non-ISDNs

Not applicable.

6.8 Protocol interactions between SS-CTAT and other supplementary services and ANFs

This clause specifies protocol interactions with other supplementary services and ANFs for which stage 3 standards had been published at the time of publication of this Standard. For interactions with supplementary services and ANFs for which stage 3 standards are published subsequent to the publication of this Standard, see those other stage 3 standards.

NOTE 6

Simultaneous conveyance of APDUs for SS-CTAT and another supplementary service or ANF in the same message, each in accordance with the requirements of its respective stage 3 standard, does not, on its own, constitute a protocol interaction.

6.8.1 Interaction with Cordless Terminal Location Registration (SS-CTLR)

The following interaction shall apply if SS-CTLR is supported in accordance with ECMA-216.

6.8.1.1 Actions at the Previous Visitor PINX

When the Previous Visitor PINX has received a pisnEnquiry invoke APDU from the Visitor PINX during CTLR and when either the authentication parameters or generated challenge(s) and the expected response value(s) for this PISN number are available, the element ctatParamInfo may be included in a transferAuthParam invoke APDU in the same message as the pisnEnquiry result APDU.

6.8.1.2 Actions at the Visitor PINX

When the element ctatParamInfo is received in the transferAuthParam invoke APDU, the authentication information may be stored in the Visitor PINX. It may later be used by the Visitor PINX to authenticate the CTM user.

6.8.2 Interaction with Cordless Terminal Incoming Call (ANF-CTMI)

No interaction.

6.8.3 Interaction with Calling Name Identification Presentation (SS-CNIP)

No interaction.

6.8.4 Interaction with Connected Name Identification Presentation (SS-CONP)

No interaction.

6.8.5 Interaction with Call Forwarding Unconditional (SS-CFU)

No interaction.

6.8.6 Interaction with Call Forwarding Busy (SS-CFB)

No interaction.

6.8.7 Interaction with Call Forwarding No Reply (SS-CFNR)

No interaction.

6.8.8 Interaction with Call Deflection (SS-CD)

No interaction.

6.8.9 Interaction with Path Replacement (ANF-PR)

No interaction.

6.8.10 Interaction with Call Transfer (SS-CT)

No interaction.

6.8.11 Interaction with Call Completion to Busy Subscriber (SS-CCBS)

No interaction.

6.8.12 Interaction with Call Completion on No Reply (SS-CCNR)

No interaction.

6.8.13 Interaction with Call Offer (SS-CO)

No interaction.

6.8.14 Interaction with Do Not Disturb (SS-DND)

No interaction.

6.8.15 Interaction with Do Not Disturb Override (SS-DNDO)

No interaction.

6.8.16 Interaction with Call Intrusion (SS-CI)

No interaction.

6.8.17 Interaction with Call Interception (ANF-CINT)

No interaction.

6.8.18 Interaction with Recall (SS-RE)

No interaction.

6.8.19 Interaction with Advice Of Charge (SS-AOC)

No interaction.

6.8.20 Interaction with Authentication of the PISN (SS-CTAN)

No interaction.

6.8.21 Interaction with Cordless Terminal Outgoing Call (ANF-CTMO)

No interaction.

6.8.22 Interaction with Message Waiting Indication (SS-MWI)

No interaction.

6.9 SS-CTAT parameter values (timers)

The following timers apply:

6.9.1 Timer T1

Timer T1 operates at the Home PINX during state CtatHomeInitiating. Its purpose is to protect against the absence of a response to the authCtmUser invoke APDU.

Timer T1 shall have a value not less than 15 s.

6.9.2 Timer T2

Timer T2 operates at the Home PINX during state CtatHomeFetching. Its purpose is to protect against the absence of a response to the ctatParamEnq invoke APDU.

Timer T2 shall have a value not less than 15 s.

6.9.3 Timer T3

Timer T3 operates at the Visitor PINX during state CtatVisitRequesting. Its purpose is to protect against the absence of a response to the getCtatParam invoke APDU.

Timer T3 shall have a value not less than 15 s.

7 Signalling protocol for the support of SS-CTAN

7.1 SS-CTAN description

SS-CTAN is a supplementary service which enables the CTM user, as a security measure, to validate the identity of the PISN, prior to accepting certain instructions from it. This is done by sending specific information to the PISN and awaiting a response. In the case where authentication fails, the CTM user shall be informed of the result and may then take any action as appropriate.

7.2 SS-CTAN operational requirements

7.2.1 Requirements on the Visitor PINX

Generic procedures for the call-independent control (connection-oriented) of supplementary services, as specified in ECMA-165 for an Originating PINX, shall apply.

7.2.2 Requirements on the Home PINX

Generic procedures for the call-independent control (connection-oriented) of supplementary services, as specified in ECMA-165 for a Terminating and an Originating PINX, shall apply.

7.2.3 Requirements on the Authentication Server PINX

Generic procedures for the call-independent control (connection-oriented) of supplementary services, as specified in ECMA-165 for a Terminating PINX, shall apply.

7.2.4 Requirements on a Transit PINX

Generic procedures for the call-independent control (connection-oriented) of supplementary services, as specified in ECMA-165 for a Transit PINX, shall apply.

7.3 SS-CTAN coding requirements

7.3.1 Operations

The operations getCtanParam and ctanParamEnq defined in the Abstract Syntax Notation number 1 (ASN.1) in table 1 in 6.3.1 shall apply to SS-CTAN.

7.3.2 Information elements

7.3.2.1 Facility information element

The operations defined in 7.3.1 shall be coded in the Facility information element in accordance with ECMA-165.

When conveying the invoke APDU of operations defined in 7.3.1, the destinationEntity data element of the NFE shall contain value endPINX.

When conveying the invoke APDU of operations defined in 7.3.1, the interpretation APDU shall either be omitted or be included with the value rejectAnyUnrecognizedInvokePdu.

7.3.2.2 Other information elements

Any other information elements (e.g. Calling party number, Called party number) shall be coded in accordance with ECMA-165.

7.3.3 Messages

The Facility information element shall be conveyed in the messages as specified in clause 10 of ECMA-165.

7.4 SS-CTAN state definitions

7.4.1 States at the Visitor PINX

The procedures for the Visitor PINX are written in terms of the following conceptual states existing within the SS-CTAN Supplementary Service Control entity in that PINX in association with a particular request for authentication of a PISN.

7.4.1.1 State CtanVisitRequestIdle

SS-CTAN is not in progress.

7.4.1.2 State CtanVisitRequesting

A getCtanParam invoke APDU has been sent.

7.4.2 States at the Home PINX

The procedures for the Home PINX are written in terms of the following conceptual states existing within the SS-CTAN Supplementary Service Control entity in that PINX in association with a particular request for authentication of a PISN.

7.4.2.1 State CtanHomeRequestIdle

Ready for receipt of a getCtanParam invoke APDU.

7.4.2.2 State CtanHomeFetching

A ctanParamEnq invoke APDU has been sent.

7.4.3 States at the Authentication Server PINX

The procedures for the Authentication Server PINX are written in terms of the following conceptual states existing within the SS-CTAN Supplementary Service Control entity in that PINX in association with a particular request for authentication of a PISN.

7.4.3.1 State CtanAuthenticationIdle

Ready for receipt of a ctanParamEnq invoke APDU.

7.5 SS-CTAN signalling procedures

Examples of message sequences are shown in annex B.

7.5.1 Actions at the Visitor PINX

The SDL representation of procedures at the Visitor PINX is shown in C.7 of annex C.

These procedures apply only when the Visitor PINX does not already have authentication parameters available for carrying out SS-CTAN.

7.5.1.1 Normal procedures

On receipt of a valid authentication request from the CTM user and in order to make a request to the Home PINX to get the authentication parameters for this CTM user, the Visitor PINX shall send a getCtanParam invoke APDU to the Home PINX containing the challenge and Authentication algorithm which was received from the CTM user and using the call reference of a call-independent signalling connection. If the Visitor PINX is able to compute a response value, the element canCompute shall be included in the getCtanParam invoke APDU. The call-independent signalling connection shall be established (or used, if an appropriate connection is already available) in accordance with the procedures specified in 7.3 of ECMA-165. The Visitor PINX shall enter state CtanVisitRequesting and start timer T4.

On receipt of the getCtanParam return result APDU, the Visitor PINX shall stop timer T4. The element ctanParamInfo contains either the authentication session key for the CTM user or the calculated response value. If it contains the authentication session key, the Visitor PINX shall use them and the challenge received from the CTM user to compute the response value for sending to the CTM user in acceptance of the authentication request. If the return result APDU contains the calculated response value, this value shall be used for sending to the CTM user in acceptance of the authentication request. The Visitor PINX shall enter state CtanVisitRequestIdle.

The Visitor PINX is responsible for clearing the call-independent signalling connection towards the Home PINX. This may occur on receipt of a return result APDU. Alternatively, the signalling connection may be retained for other applications, if appropriate.

7.5.1.2 Exceptional procedures

On receipt of a getCtanParam return error or reject APDU from the Home PINX, the Visitor PINX shall stop timer T4. A response shall be sent to the CTM user indicating rejection of the authentication request, and the Visitor PINX shall enter state CtanVisitRequestIdle.

If timer T4 expires (i.e. the getCtanParam invoke APDU is not answered by the Home PINX), a response shall be sent to the CTM user indicating rejection of the authentication request, and the Visitor PINX shall enter state CtanVisitRequestIdle.

The Visitor PINX is responsible for clearing the call-independent signalling connection towards the Home PINX. This may occur on receipt of a return error or reject APDU or on expiry of timer T4. Alternatively, the signalling connection may be retained for other applications, if appropriate.

7.5.2 Actions at the Home PINX

The SDL representation of procedures at the Home PINX is shown in C.8 of annex C.

When a Home PINX also provides Authentication Server PINX functionality, the joint requirements of 7.5.2 (for a Home PINX) and 7.5.3 (for an Authentication Server PINX) shall apply, with the exception that any communication between the Home PINX functionality and the Authentication Server PINX functionality will be an intra-PINX matter. The messages specified for sending from the Home PINX towards the Authentication Server PINX or vice versa will not appear on any inter-PINX link.

7.5.2.1 Normal procedures

On receipt of a getCtanParam invoke APDU using the call reference of a call-independent signalling connection (as specified in 7.3 of ECMA-165), the Home PINX shall check that the received PISN number of the CTM user is valid and that the CTM user is authorised for the SS-CTAN. If authorized the Home PINX shall then send a ctanParamEnq invoke APDU to the Authentication Server PINX, containing the received challenge and using the call reference of a call-independent signalling connection. The call-independent signalling connection shall be established (or used, if an appropriate connection is already available) in accordance with the procedures specified in 7.3 of ECMA-165. The Home PINX shall enter state CtanHomeFetching and start timer T5.

On receipt of the ctanParamEnq return result APDU, the Home PINX shall stop timer T5 and answer the getCtanParam invoke APDU with a return result APDU containing the information received in the ctanParamEnq return result APDU. The Home PINX shall enter state CtanHomeRequestIdle.

The Home PINX is responsible for clearing the call-independent signalling connection towards the Authentication Server PINX. This may occur on receipt of a return result APDU. Alternatively, the signalling connection may be retained for other applications, if appropriate.

7.5.2.2 Exceptional procedures

If the received PISN number is not valid, the Home PINX shall answer the getCtanParam invoke APDU with a return error APDU containing the error invalidServedUserNr and remain in state CtanHomeRequestIdle.

If the CTM user is not authorised for SS-CTAN, the Home PINX shall answer the getCtanParam invoke APDU with a return error APDU containing the error notAuthorized and remain in state CtanHomeRequestIdle.

On receipt of a ctanParamEnq return error APDU from the Authentication Server PINX, the Home PINX shall stop timer T5 and answer the getCtanParam invoke APDU with a return error APDU containing the received error value and enter state CtanHomeRequestIdle.

On receipt of a reject APDU from the Authentication Server PINX, the Home PINX shall stop timer T5 and answer the getCtanParam invoke APDU with a return error APDU containing the error paramNotAvailable and enter state CtanHomeRequestIdle.

If timer T5 expires (i.e. the ctanParamEnq invoke APDU is not answered by the Authentication Server PINX), the Home PINX shall answer the getCtanParam invoke APDU with a return error APDU containing the error value temporarilyUnavailable and enter state CtanHomeRequestIdle.

The Home PINX is responsible for clearing the call-independent signalling connection towards the Authentication Server PINX. This may occur on receipt of a return error or reject APDU or on expiry of timer T5. Alternatively, the signalling connection may be retained for other applications, if appropriate.

7.5.3 Actions at the Authentication Server PINX

The SDL representation of procedures at the Authentication Server PINX is shown in C.9 of annex C.

7.5.3.1 Normal procedures

On receipt of a ctanParamEnq invoke APDU using the call reference of a call-independent signalling connection (as specified in 7.3 of ECMA-165), the Authentication Server PINX shall check that the received PISN number of the CTM user is valid and retrieve the authentication parameters if available. If it is required by the application or if the element canCompute is not included in the ctanParamEnq invoke APDU, the Authentication Server PINX shall use the received challenge to compute a response value and answer the ctanParamEnq invoke APDU with a return result APDU where element ctanParamInfo contains the calculated response value (choice calcCtanInfo). If the element canCompute is included in the ctanParamEnq invoke APDU and if it is not required by the application to compute the expected response value, the Authentication Server PINX shall answer the ctanParamEnq invoke APDU with a return result APDU where element ctanParamInfo contains the authentication session key (choice authSessionKeyInfo). The Authentication Server PINX shall remain in state CtanAuthenticationIdle.

7.5.3.2 Exceptional procedures

If the received PISN number is not valid, the Authentication Server PINX shall answer the ctanParamEnq invoke APDU with a return error APDU containing the error invalidServedUserNr and remain in state CtanAuthenticationIdle.

If the authentication parameters are not available, the Authentication Server PINX shall answer the ctanParamEnq invoke APDU with a return error APDU containing the error paramNotAvailable. The Authentication Server PINX shall remain in state CtanAuthenticationIdle.

7.5.4 Actions at a Transit PINX for authentication of a PISN

No special actions are required in support of authentication of a PISN.

7.6 SS-CTAN impact of interworking with public ISDNs

Not applicable.

7.7 SS-CTAN impact of interworking with non-ISDNs

Not applicable.

7.8 Protocol interactions between SS-CTAN and other supplementary services and ANFs

This clause specifies protocol interactions with other supplementary services and ANFs for which stage 3 standards had been published at the time of publication of this Standard. For interactions with supplementary services and ANFs for which stage 3 standards are published subsequent to the publication of this Standard, see those other stage 3 standards.

NOTE 7

Simultaneous conveyance of APDUs for SS-CTAN and another supplementary service or ANF in the same message, each in accordance with the requirements of its respective stage 3 standard, does not, on its own, constitute a protocol interaction.

7.8.1 Interaction with Cordless Terminal Location Registration (SS-CTLR)

No interaction.

7.8.2 Interaction with Cordless Terminal Incoming Call (ANF-CTMI)

No interaction.

7.8.3 Interaction with Calling Name Identification Presentation (SS-CNIP)

No interaction.

7.8.4 Interaction with Connected Name Identification Presentation (SS-CONP)

No interaction.

7.8.5 Interaction with Call Forwarding Unconditional (SS-CFU)

No interaction.

7.8.6 Interaction with Call Forwarding Busy (SS-CFB)

No interaction.

7.8.7 Interaction with Call Forwarding No Reply (SS-CFNR)

No interaction.

7.8.8 Interaction with Call Deflection (SS-CD)

No interaction.

7.8.9 Interaction with Path Replacement (ANF-PR)

No interaction.

7.8.10 Interaction with Call Transfer (SS-CT)

No interaction.

7.8.11 Interaction with Call Completion to Busy Subscriber (SS-CCBS)

No interaction.

7.8.12 Interaction with Call Completion on No Reply (SS-CCNR)

No interaction.

7.8.13 Interaction with Call Offer (SS-CO)

No interaction.

7.8.14 Interaction with Do Not Disturb (SS-DND)

No interaction.

7.8.15 Interaction with Do Not Disturb Override (SS-DNDO)

No interaction.

7.8.16 Interaction with Call Intrusion (SS-CI)

No interaction.

7.8.17 Interaction with Call Interception (ANF-CINT)

No interaction.

7.8.18 Interaction with Recall (SS-RE)

No interaction.

7.8.19 Interaction with Advice Of Charge (SS-AOC)

No interaction.

7.8.20 Interaction with Authentication of a CTM user (SS-CTAT)

No interaction.

7.8.21 Interaction with Cordless Terminal Outgoing Call (ANF-CTMO)

No interaction.

7.8.22 Interaction with Message Waiting Indication (SS-MWI)

No interaction.

7.9 SS-CTAN parameter values (timers)

The following timers apply:

7.9.1 Timer T4

Timer T4 operates at the Visitor PINX during state CtanVisitRequesting. Its purpose is to protect against the absence of a response to the getCtanParam invoke APDU.

Timer T4 shall have a value not less than 15 s.

7.9.2 Timer T5

Timer T5 operates at the Home PINX during state CtanHomeFetching. Its purpose is to protect against the absence of a response to the ctanParamEnq invoke APDU.

Timer T5 shall have a value not less than 15 s.

Annex A

(normative)

Protocol Implementation Conformance Statement (PICS) Proforma

A.1 Introduction

The supplier of a protocol implementation which is claimed to conform to this Standard shall complete the following Protocol Implementation Conformance Statement (PICS) proforma.

A completed PICS proforma is the PICS for the implementation in question. The PICS is a statement of which capabilities and options of the protocol have been implemented. The PICS can have a number of uses, including use:

- by the protocol implementor, as a check-list to reduce the risk of failure to conform to the Standard through oversight;
- by the supplier and acquirer, or potential acquirer, of the implementation, as a detailed indication of the capabilities of the implementation, stated relative to the common basis for understanding provided by the Standard's PICS proforma;
- by the user or potential user of the implementation, as a basis for initially checking the possibility of interworking with another implementation - while interworking can never be guaranteed, failure to interwork can often be predicted from incompatible PICSs;
- by a protocol tester, as the basis for selecting appropriate tests against which to assess the claim for conformance of the implementation.

A.2 Instructions for completing the PICS proforma

A.2.1 General structure of the PICS proforma

The PICS proforma is a fixed-format questionnaire divided into sub-clauses each containing a group of individual items. Each item is identified by an item number, the name of the item (question to be answered), and the reference(s) to the clause(s) that specifies (specify) the item in the main body of this Standard.

The "Status" column indicates whether an item is applicable and, if so, whether support is mandatory or optional.

The following terms are used:

m	mandatory (the capability is required for conformance to the protocol);
o	optional (the capability is not required for conformance to the protocol, but if the capability is implemented it is required to conform to the protocol specifications);
o.<n>	optional, but support of at least one of the group of options labelled by the same numeral <n> is required;
x	prohibited;
c.<cond>	conditional requirement, depending on support for the item or items listed in condition <cond>;
<item>:m	simple conditional requirement, the capability being mandatory if item number <item> is supported, otherwise not applicable;
<item>:o	simple conditional requirement, the capability being optional if item number <item> is supported, otherwise not applicable.

Answers to the questionnaire items are to be provided either in the "Support" column, by simply marking an answer to indicate a restricted choice (Yes or No), or in the "Not Applicable" column (N/A).

A.2.2 Additional information

Items of additional information allow a supplier to provide further information intended to assist the interpretation of the PICS. It is not intended or expected that a large quantity will be supplied, and a PICS can be considered complete without any such information. Examples might be an outline of the ways in which a (single) implementation can be set up to operate in a variety of environments and configurations.

References to items of additional information may be entered next to any answer in the questionnaire, and may be included in items of exception information.

A.2.3 Exception information

It may occasionally happen that a supplier will wish to answer an item with mandatory or prohibited status (after any conditions have been applied) in a way that conflicts with the indicated requirement. No pre-printed answer will be found in the Support column for this. Instead, the supplier is required to write into the Support column an x.<i> reference to an item of exception information, and to provide the appropriate rationale in the exception item itself.

An implementation for which an exception item is required in this way does not conform to this Standard. A possible reason for the situation described above is that a defect in the Standard has been reported, a correction for which is expected to change the requirement not met by the implementation.

A.3 PICS proforma for SS-CTAT

A.3.1 Implementation identification

Supplier	
Contact point for queries about the PICS	
Implementation name(s) and version(s)	
Other information necessary for full identification, e.g. name(s) and version(s) for machines and/or operating systems; system name(s)	

Only the first three items are required for all implementations; other information may be completed as appropriate in meeting the requirement for full identification.

The terms name and version should be interpreted appropriately to correspond with a supplier's terminology (e.g. type, series, model).

A.3.2 Protocol summary

Protocol version	1.0
Addenda implemented (if applicable)	
Amendments implemented	
Have any exception items been required (see A.2.3)?	No [ ] Yes [ ] (The answer Yes means that the implementation does not conform to this Standard)

Date of Statement	

A.3.3 General

Item	Question/feature	References	Status	N/A	Support
A1	Behaviour as Visitor PINX for SS-CTAT		o.1		Yes [ ] No [ ]
A2	Behaviour as Home PINX for SS-CTAT (separate from an Authentication Server PINX)		o.1		Yes [ ] No [ ]
A3	Behaviour as combined Home PINX and Authentication Server PINX		o.1		Yes [ ] No [ ]
A4	Behaviour as Authentication Server PINX for SS-CTAT (separate from a Home PINX)		o.1		Yes [ ] No [ ]

A.3.4 Procedures

Item	Question/feature	References	Status	N/A	Support
B1	Support of ECMA-165 procedures at a Visitor PINX	6.2.1	A1:m	[ ]	m: Yes [ ]
B2	Support of ECMA-165 procedures at a Home PINX	6.2.2	c.1	[ ]	m: Yes [ ]
B3	Support of ECMA-165 procedures at an Authentication Server PINX	6.2.3	A4:m	[ ]	m: Yes [ ]
B4	Signalling procedures at a Visitor PINX for receiving request from Home PINX for SS-CTAT with challenge and expected response	6.5.5	A1:m	[ ]	m: Yes [ ]
B5	Signalling procedures at a Visitor PINX for receiving request from Home PINX for SS-CTAT without challenge and expected response	6.5.5	A1:o	[ ]	Yes [ ] No [ ]
B6	Support of procedures for initiation of SS-CTAT at the Visitor PINX	6.5.4	A1:o	[ ]	Yes [ ] No [ ]
B7	Signalling procedures at a Visitor PINX for requesting authentication parameters from Home PINX	6.5.6	c.2	[ ]	m: Yes [ ]
B8	Support of procedures for calculation of challenge/response at the Visitor PINX	6.5.6	A1:o	[ ]	Yes [ ] No [ ]
B9	Signalling procedures at a Home PINX for initiation of SS-CTAT without challenge and expected response	6.5.1	c.3	[ ]	Yes [ ] No [ ]
B10	Signalling procedures at a Home PINX for initiation of SS-CTAT with challenge and expected response	6.5.1	c.1	[ ]	m: Yes [ ]
B11	Signalling procedures at a Home PINX for receiving request from Visitor PINX for authentication parameters	6.5.2	c.1	[ ]	m: Yes [ ]
B12	Signalling procedures at a Home PINX for fetching authentication parameters from Authentication Server PINX	6.5.3	A2:m	[ ]	m: Yes [ ]

B13	Signalling procedures at an Authentication Server PINX	6.5.7	A4:m	[ ]	m: Yes [ ]

c.1: if A2 or A3 then mandatory, else N/A

c.2: if B5 or B6 then mandatory, else N/A

c.3: if A2 or A3 then optional, else N/A

A.3.5 Coding

Item	Question/feature	References	Status	N/A	Support
C1	Sending of authCtmUser invoke APDU and receipt of return result and return error APDUs	6.3	c.4	[ ]	m: Yes [ ]
C2	Sending of getCtatParam invoke APDU and receipt of return result and return error APDUs	6.3	B7:m	[ ]	m: Yes [ ]
C3	Sending of ctatParamEnq invoke APDU and receipt of return result and return error APDUs	6.3	A2:m	[ ]	m: Yes [ ]
C4	Receipt of authCtmUser invoke APDU and sending of return result and return error APDUs	6.3	c.5	[ ]	m: Yes [ ]
C5	Receipt of getCtatParam invoke APDU and sending of return result and return error APDUs	6.3	B11:m	[ ]	m: Yes [ ]
C6	Receipt of ctatParamEnq invoke APDU and sending of return result and return error APDUs	6.3	A4:m	[ ]	m: Yes [ ]

c.4: if B9 or B10 then mandatory, else N/A

c.5: if B4 or B5 then mandatory, else N/A

A.3.6 Timers

Item	Question/feature	References	Status	N/A	Support
D1	Support of timer T1	6.9.1	c.6	[ ]	m: Yes [ ] Value [. . . .]
D2	Support of timer T2	6.9.2	A2:m	[ ]	m: Yes [ ] Value [. . . .]
D3	Support of timer T3	6.9.3	B7:m	[ ]	m: Yes [ ] Value [. . . .]

c.6: if B9 or B10 then mandatory, else N/A

A.3.7 Interactions between SS-CTAT and SS-CTLR

Item	Question/feature	References	Status	N/A	Support
E1	Support of SS-CTLR		o		Yes [ ] No [ ]
E2	Interactions at Previous Visitor PINX	6.8.1.1	c.7	[ ]	Yes [ ] No [ ]
E3	Interactions at Visitor PINX	6.8.1.2	c.7	[ ]	Yes [ ] No [ ]

c.7: if E1 then optional, else N/A

A.4 PICS proforma for SS-CTAN

A.4.1 Implementation identification

Supplier	
Contact point for queries about the PICS	
Implementation name(s) and version(s)	
Other information necessary for full identification, e.g. name(s) and version(s) for machines and/or operating systems; system name(s)	

Only the first three items are required for all implementations; other information may be completed as appropriate in meeting the requirement for full identification.

The terms name and version should be interpreted appropriately to correspond with a supplier's terminology (e.g. type, series, model).

A.4.2 Protocol summary

Protocol version	1.0
Addenda implemented (if applicable)	
Amendments implemented	
Have any exception items been required (see A.2.3)?	No [ ] Yes [ ] (The answer Yes means that the implementation does not conform to this Standard)

Date of Statement	

A.4.3 General

Item	Question/feature	References	Status	N/A	Support
A1	Behaviour as Visitor PINX for SS-CTAN		o.1		Yes [ ] No [ ]
A2	Behaviour as Home PINX for SS-CTAN (separate from an Authentication Server PINX)		o.1		Yes [ ] No [ ]
A3	Behaviour as combined Home PINX and Authentication Server PINX		o.1		Yes [ ] No [ ]
A4	Behaviour as Authentication Server PINX for SS-CTAN (separate from a Home PINX)		o.1		Yes [ ] No [ ]

A.4.4 Procedures

Item	Question/feature	References	Status	N/A	Support
B1	Support of ECMA-165 procedures at a Visitor PINX	7.2.1	A1:m	[ ]	m: Yes [ ]
B2	Support of ECMA-165 procedures at a Home PINX	7.2.2	c.1	[ ]	m: Yes [ ]
B3	Support of ECMA-165 procedures at an Authentication Server PINX	7.2.3	A4:m	[ ]	m: Yes [ ]
B4	Signalling procedures at a Visitor PINX	7.5.1	A1:m	[ ]	m: Yes [ ]
B5	Support of procedures for calculation of response value at the Visitor PINX	7.5.1	A1:o	[ ]	Yes [ ] No [ ]
B6	Signalling procedures at a Home PINX for receiving request from Visitor PINX for authentication parameters	7.5.2	c.1	[ ]	m: Yes [ ]
B7	Signalling procedures at a Home PINX for fetching authentication parameters from Authentication Server PINX	7.5.2	A2:m	[ ]	m: Yes [ ]
B8	Signalling procedures at an Authentication Server PINX	7.5.3	A4:m	[ ]	m: Yes [ ]

c.1: if A2 or A3 then mandatory, else N/A

A.4.5 Coding

Item	Question/feature	References	Status	N/A	Support
C1	Sending of getCtanParam invoke APDU and receipt of return result and return error APDUs	7.3	A1:m	[ ]	m: Yes [ ]
C2	Sending of ctanParamEnq invoke APDU and receipt of return result and return error APDUs	7.3	A2:m	[ ]	m: Yes [ ]
C3	Receipt of getCtanParam invoke APDU and sending of return result and return error APDUs	7.3	c.2	[ ]	m: Yes [ ]
C4	Receipt of ctanParamEnq invoke APDU and sending of return result and return error APDUs	7.3	A4:m	[ ]	m: Yes [ ]

c.2: if A2 or A3 then mandatory, else N/A

A.4.6 Timers

Item	Question/feature	References	Status	N/A	Support
D1	Support of timer T4	7.9.1	A1:m	[ ]	m: Yes [ ] Value [. . . .]
D2	Support of timer T5	7.9.2	A2:m	[ ]	m: Yes [ ] Value [. . . .]

Annex B

(informative)

Examples of Message Sequences

This annex describes some typical message flows for SS-CTAT and SS-CTAN. The following conventions are used in the figures of this annex.

1. The following notation is used:


Call-independent signalling connection message containing SS-CTAT/SS-CTAN information

Call-independent signalling connection message without SS-CTAT/SS-CTAN information

Symbolic primitive carrying SS-CTAT/SS-CTAN information

xxx.inv	Invoke APDU for operation xxx
xxx.res	Return result APDU for operation xxx
xxx.err	Return error APDU for operation xxx

2. The figures show messages exchanged via Protocol Control between PINXs involved in SS-CTAT/SS-CTAN. Only messages relevant to SS-CTAT/SS-CTAN are shown.

3. Only the relevant information content (e.g. remote operation APDUs, notifications, information elements) is listed below each message name. The Facility and Notification indicator information elements containing remote operation APDUs and notifications are not explicitly shown. Information with no impact on SS-CTAT/SS-CTAN is not shown.

4. Some interactions with users are included in the form of symbolic primitives. The actual protocol at the terminal interface is outside the scope of this Standard.

B.1 Successful authentication of a CTM user (SS-CTAT); the Visitor PINX initiates SS-CTAT

Figure B.1 shows an example message flow of successful authentication of a CTM user. The Visitor PINX initiates SS-CTAT; authentication parameters are not available in the Visitor PINX. The Authentication Server PINX is the Home PINX.

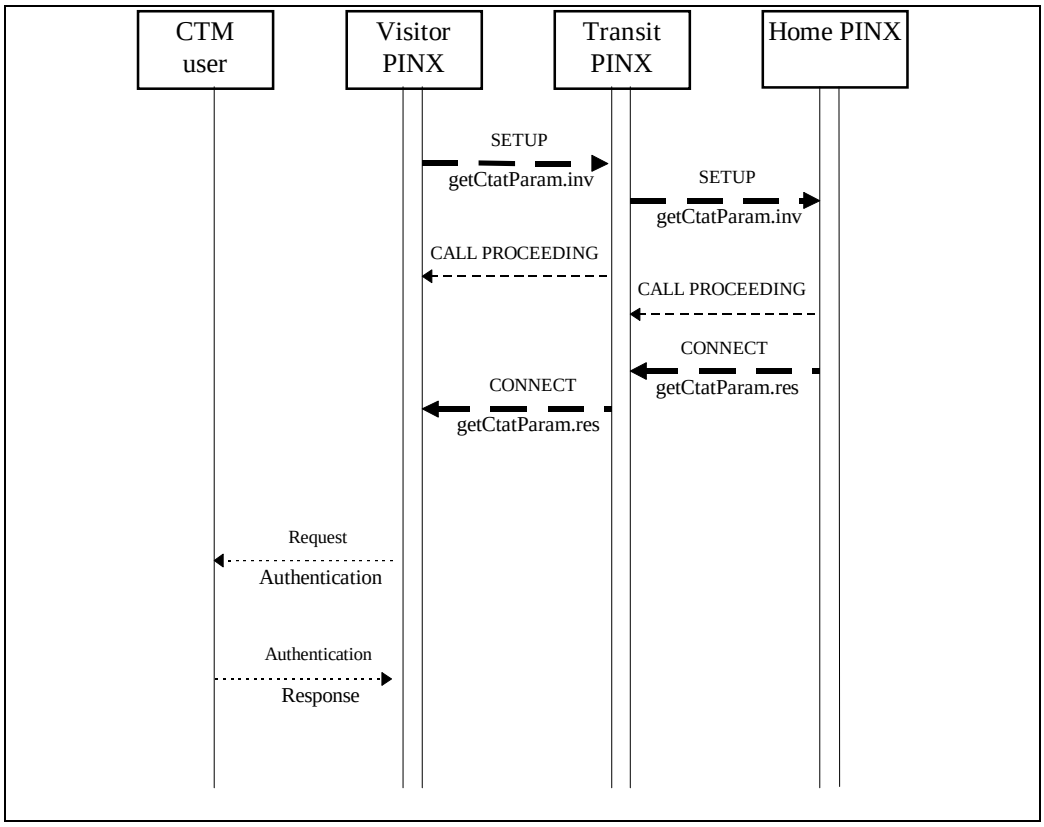

Figure B.1 - Example message flow for authentication of a CTM user

B.2 Successful authentication of a CTM user (SS-CTAT); the Home PINX initiates SS-CTAT without including challenge and response values

Figure B.2 shows an example message flow of successful authentication of a CTM user. The Home PINX initiates SS-CTAT without including challenge and response values; authentication parameters are not available in the Visitor PINX. The Authentication Server PINX is not the Home PINX.

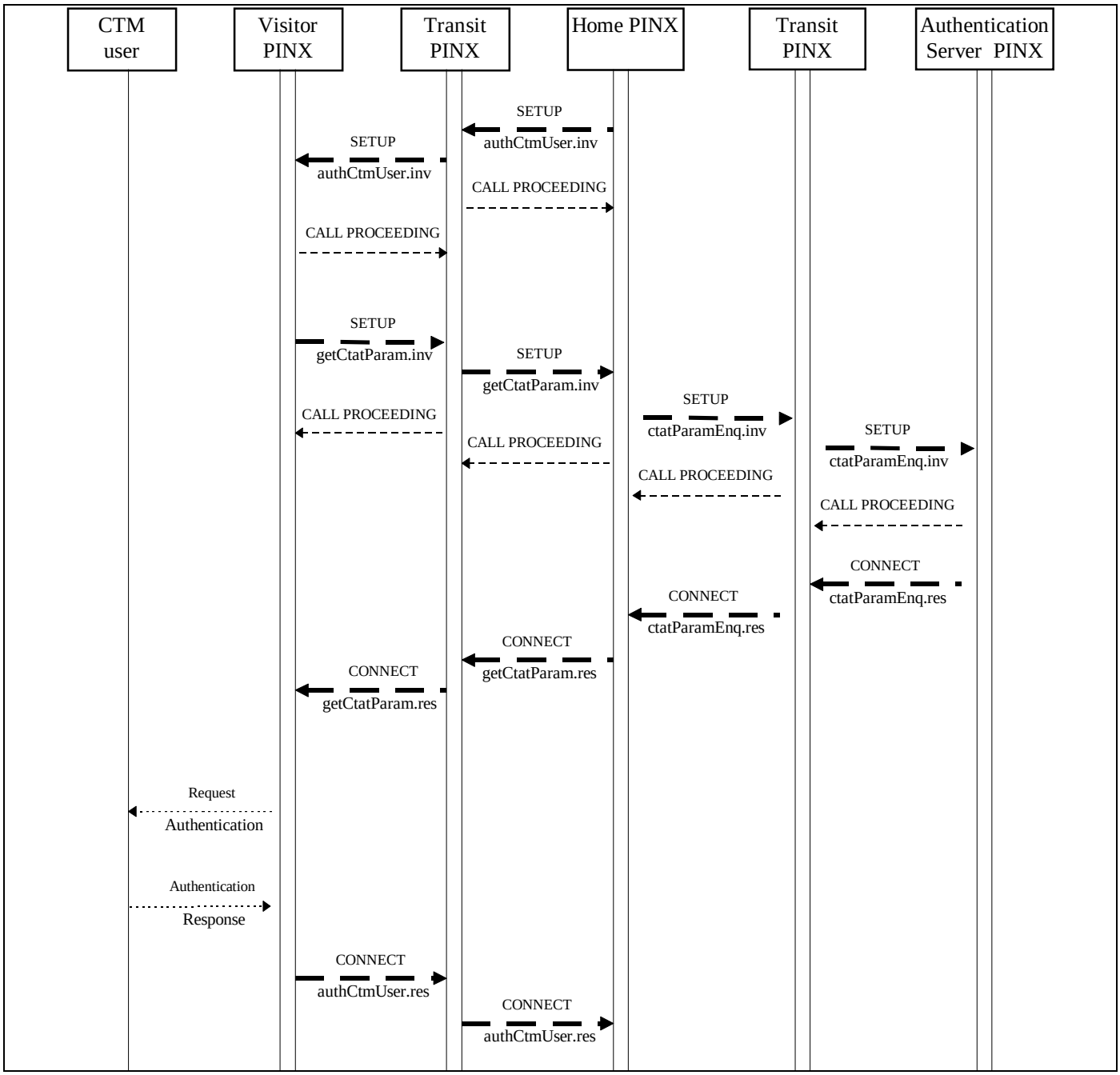

Figure B.2 - Example message flow for authentication of a CTM user

B.3 Successful authentication of a CTM user (SS-CTAT); the Home PINX initiates SS-CTAT with challenge and response values included

Figure B.3 shows an example message flow of successful authentication of a CTM user. The Home PINX initiates SS-CTAT with challenge and response values included. The Authentication Server PINX is not the Home PINX.

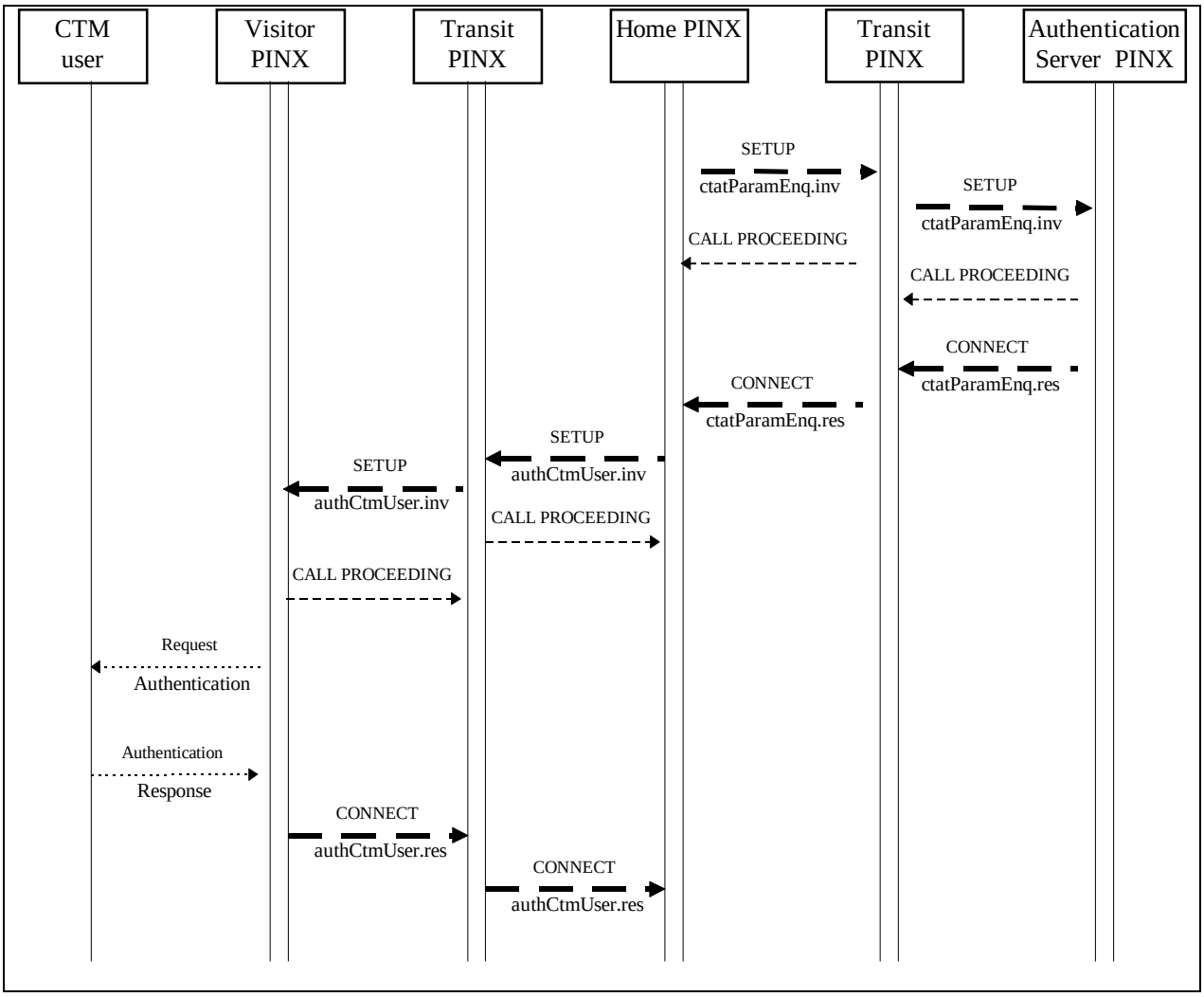

Figure B.3 - Example message flow for authentication of a CTM user

B.4 Successful authentication of a PISN (SS-CTAN); parameters retrieved from Home PINX

Figure B.4 shows an example message flow of successful authentication of a PISN. The Authentication Server PINX is not the Home PINX.

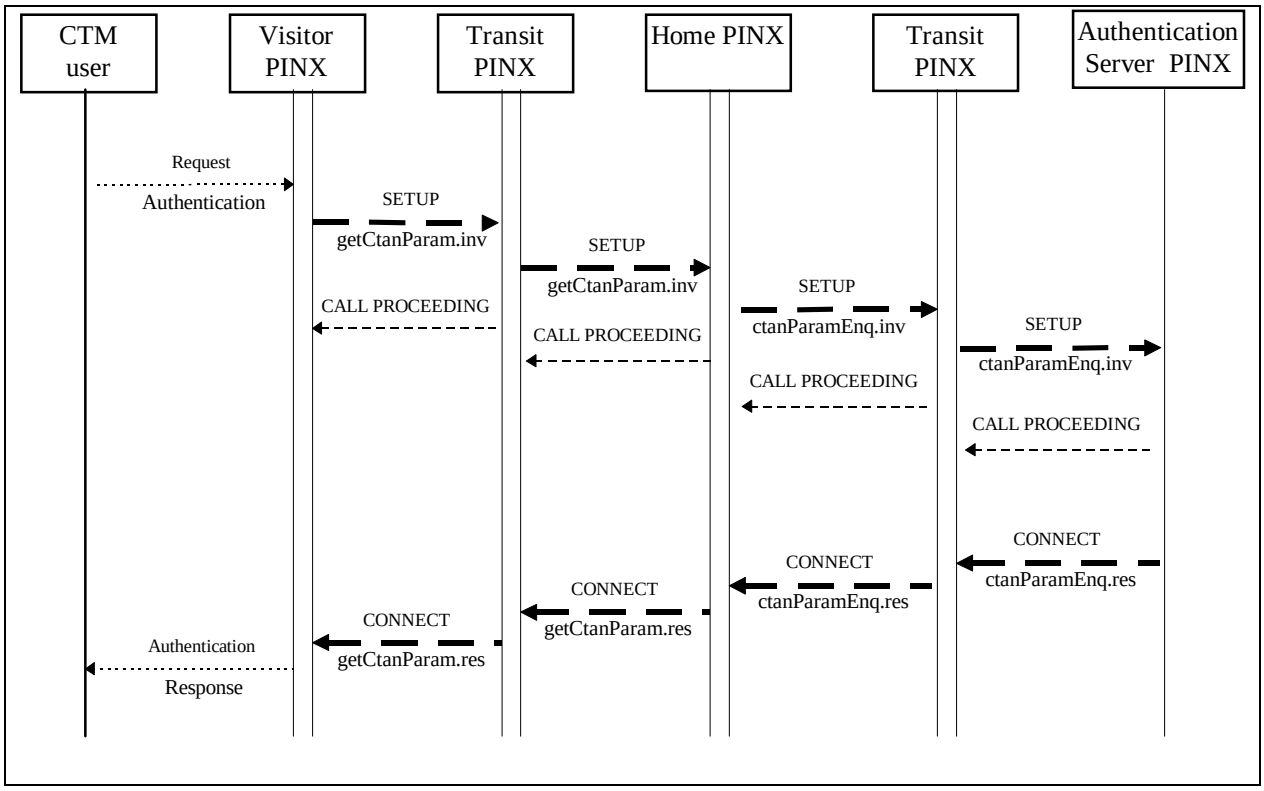

Figure B.4 - Example message flow for authentication of a PISN

Annex C

(informative)

Specification and Description Language (SDL) Representation of Procedures

The diagrams in this annex use the Specification and Description Language defined in ITU-T Rec. Z.100 (1993).

Each diagram represents the behaviour of an SS-CTAT or SS-CTAN Supplementary Service Control entity at a particular type of PINX. In accordance with the protocol model described in ECMA-165, the Supplementary Service Control entity uses, via the Coordination Function, the services of Generic Functional Procedures Control and Basic Call Control.

Where an output symbol represents a primitive to the Coordination Function, and that primitive results in a message being sent, the output symbol bears the name of the message and any remote operation APDU(s) or notification(s) contained in that message.

Where an input symbol represents a primitive from the Coordination Function, and that primitive is the result of a message being received, the input symbol bears the name of the message and any remote operation APDU(s) or notification(s) contained in that message.

The following abbreviations are used:

inv. invoke APDU

res. return result APDU

err. return error APDU

rej. reject APDU

C.1 SDL representation at the Home PINX for initiation of SS-CTAT

Figure C.1 shows the behaviour of an SS-CTAT Supplementary Service Control entity within the Home PINX for initiation of SS-CTAT.

Input signals from the left and output signals to the left represent internal primitives.

Input signals from the right and output signals to the right represent primitives to and from the Coordination Function in respect of messages sent to and received from the Visitor PINX. Also protocol timer expiry is indicated by an input signal from the right.

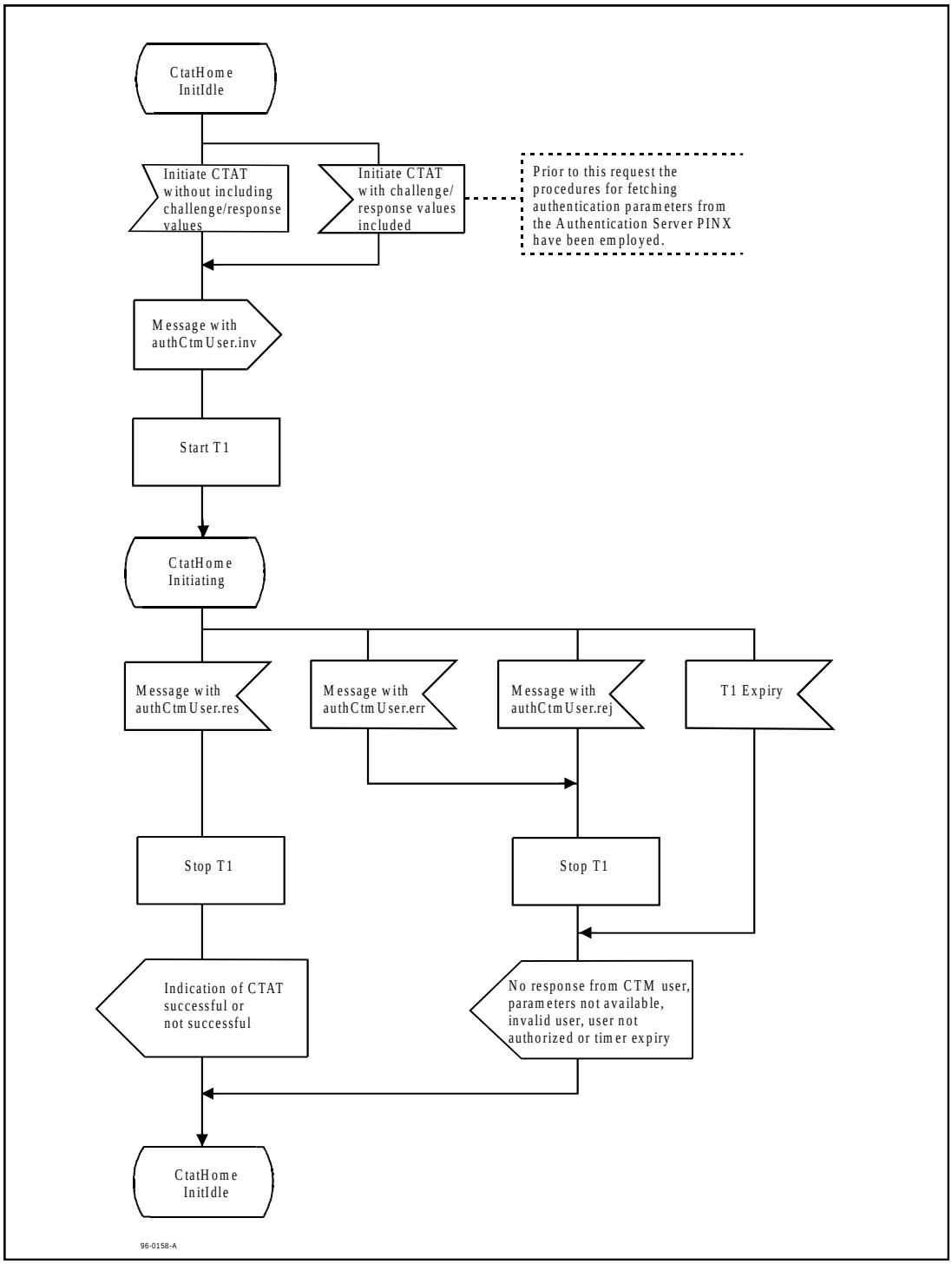

Figure C.1 - SDL representation at the Home PINX for initiation of SS-CTAT

C.2 SDL representation of SS-CTAT at the Home PINX for requesting authentication parameters

Figure C.2 shows the behaviour of an SS-CTAT Supplementary Service Control entity within the Home PINX if authentication parameters are requested by the Visitor PINX.

Input signals from the left and output signals to the left represent internal primitives.

Input signals from the right and output signals to the right represent primitives to and from the Coordination Function in respect of messages received from and sent to the Visitor PINX. Also protocol timer expiry is indicated by an input signal from the right.

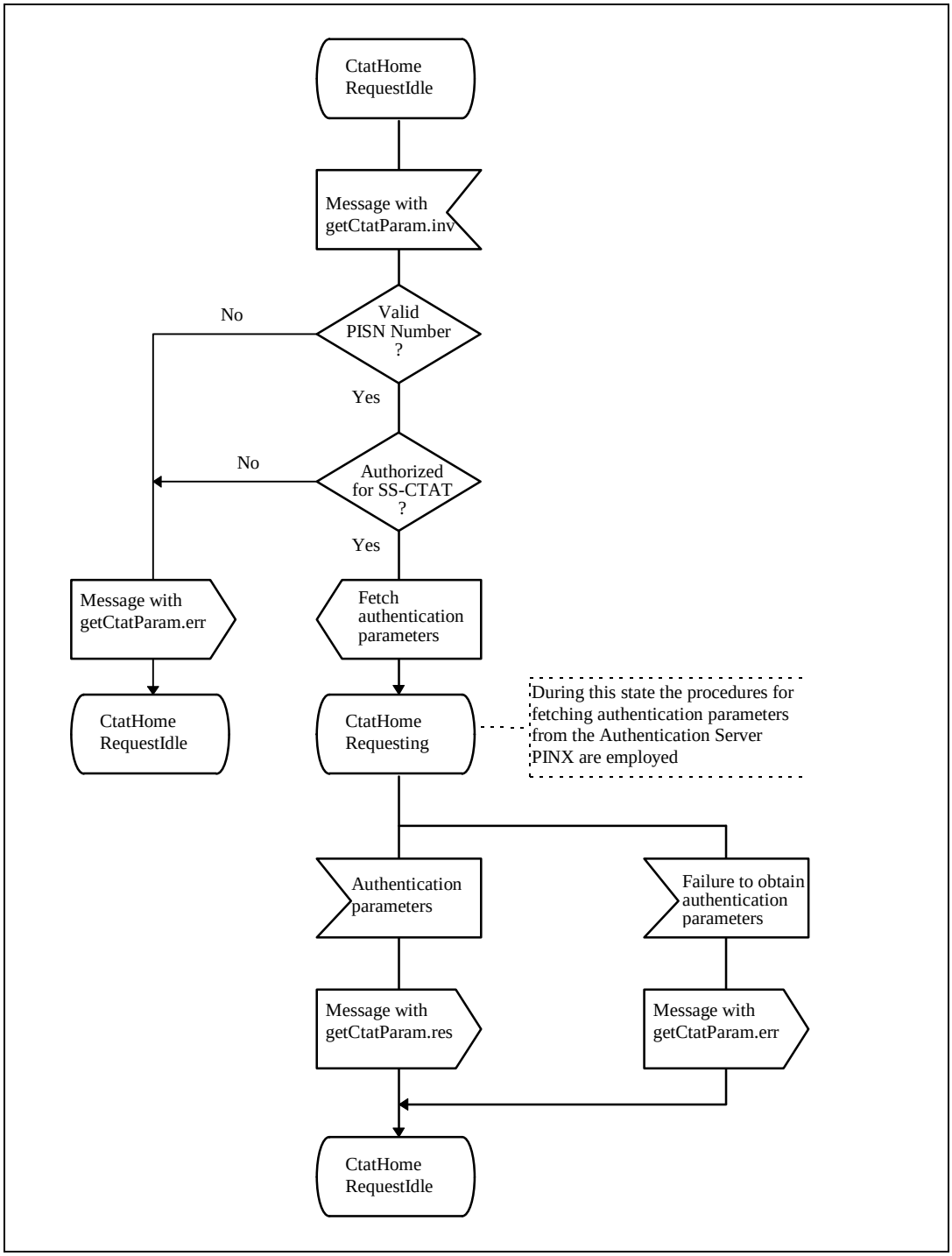

Figure C.2 - SDL representation of SS-CTAT at the Home PINX for requesting authentication parameters

C.3 SDL representation of SS-CTAT at the Home PINX when fetching authentication parameters

Figure C.3 shows the behaviour of an SS-CTAT Supplementary Service Control entity within the Home PINX when fetching authentication parameters from the Authentication Server PINX.

Input signals from the left and output signals to the left represent internal primitives.

Input signals from the right and output signals to the right represent primitives to and from the Coordination Function in respect of messages sent to and received from the Authentication Server PINX. Also protocol timer expiry is indicated by an input signal from the right.

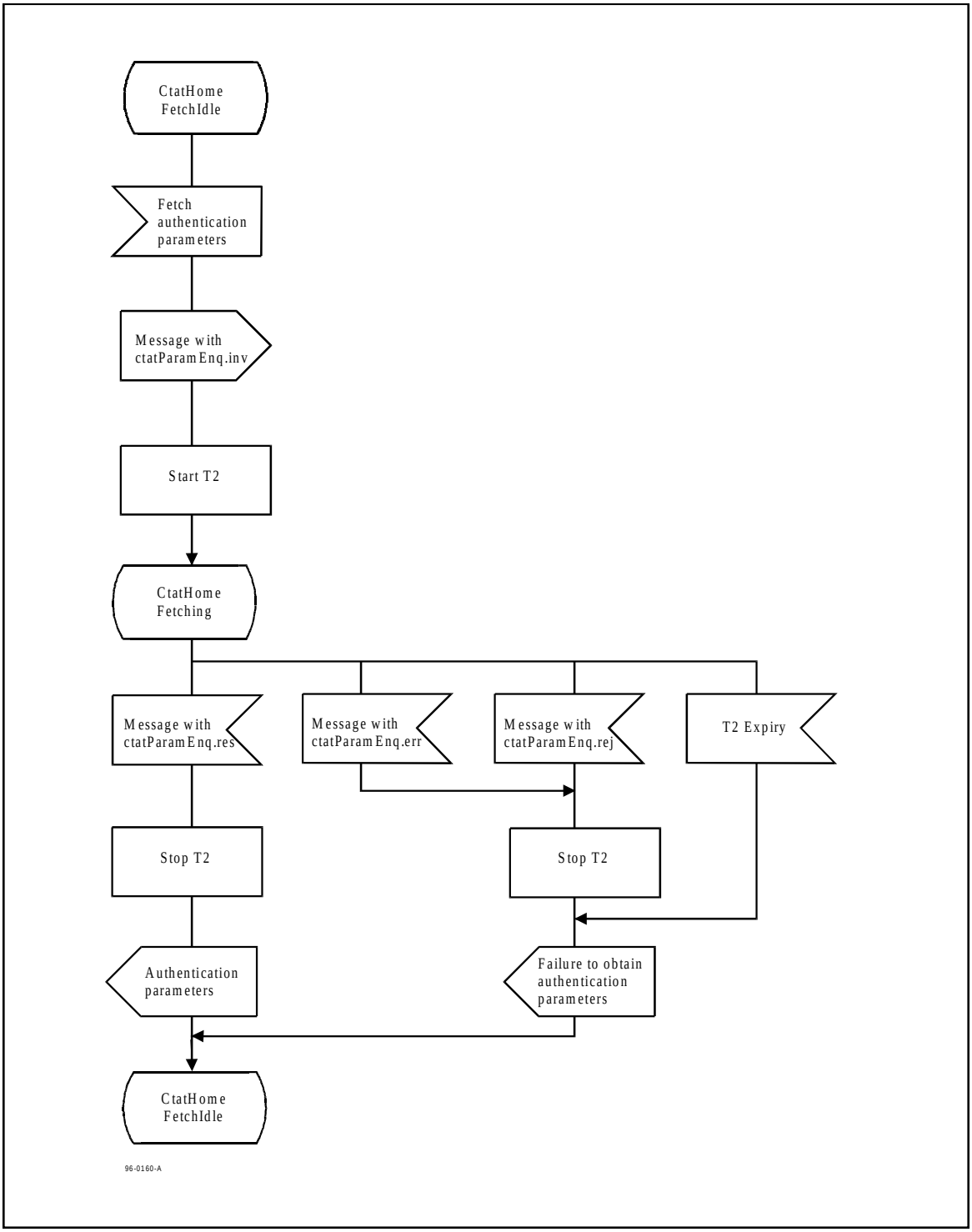

Figure C.3 - SDL representation of SS-CTAT at the Home PINX when fetching authentication parameters

C.4 SDL representation at the Visitor PINX for execution of SS-CTAT

Figure C.4 shows the behaviour of an SS-CTAT Supplementary Service Control entity within the Visitor PINX for execution of SS-CTAT.

Input signals from the left and output signals to the left represent internal primitives.

Input signals from the right and output signals to the right represent primitives to and from the Coordination Function in respect of messages received from and sent to the Home PINX. Also protocol timer expiry is indicated by an input signal from the right.

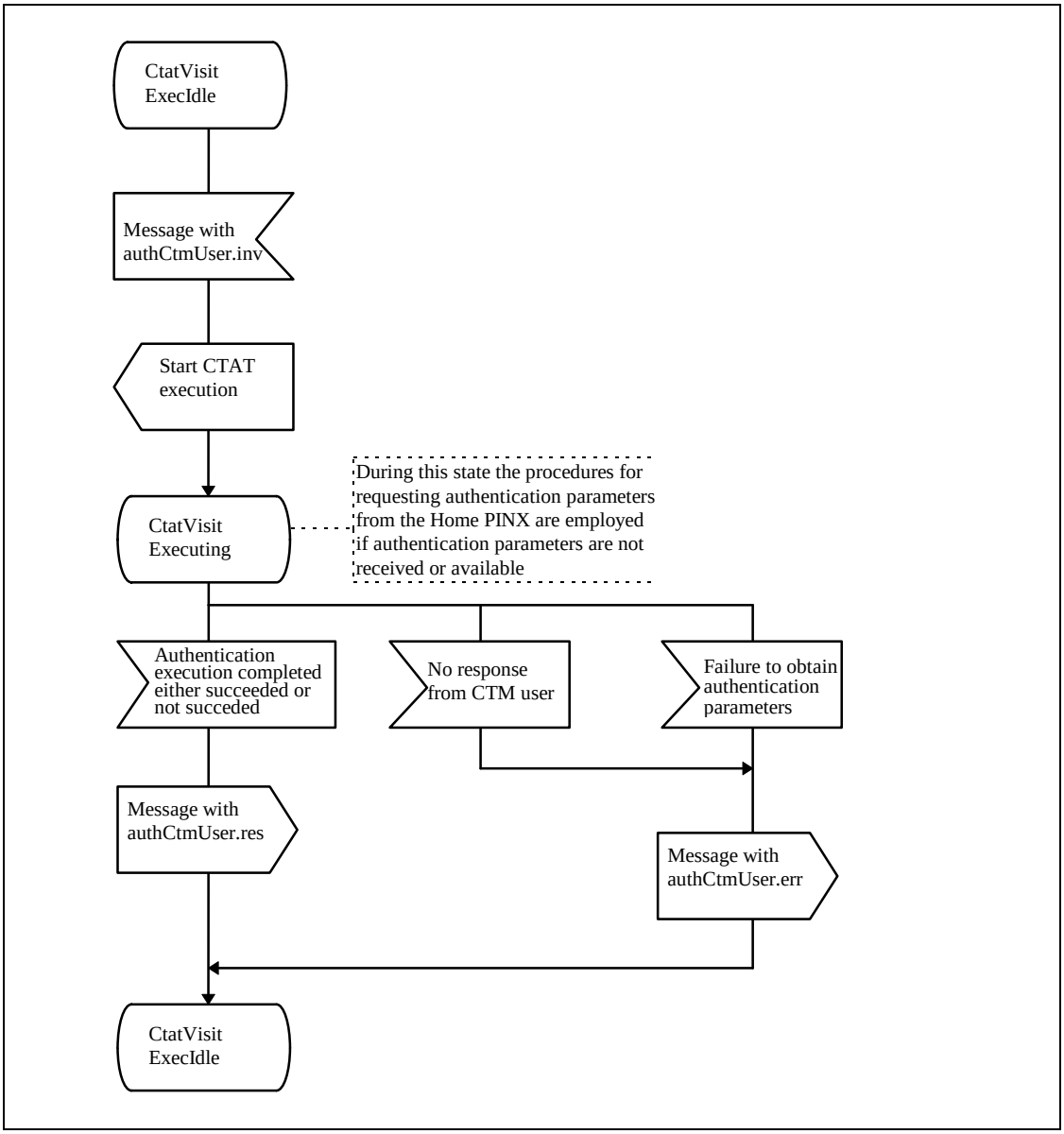

Figure C.4 - SDL representation at the Visitor PINX for execution of SS-CTAT

C.5 SDL representation of SS-CTAT at the Visitor PINX for requesting authentication parameters

Figure C.5 shows the behaviour of an SS-CTAT Supplementary Service Control entity within the Visitor PINX for requesting authentication parameters.

Input signals from the left and output signals to the left represent internal primitives.

Input signals from the right and output signals to the right represent primitives to and from the Coordination Function in respect of messages sent to and received from the Home PINX. Also protocol timer expiry is indicated by an input signal from the right.

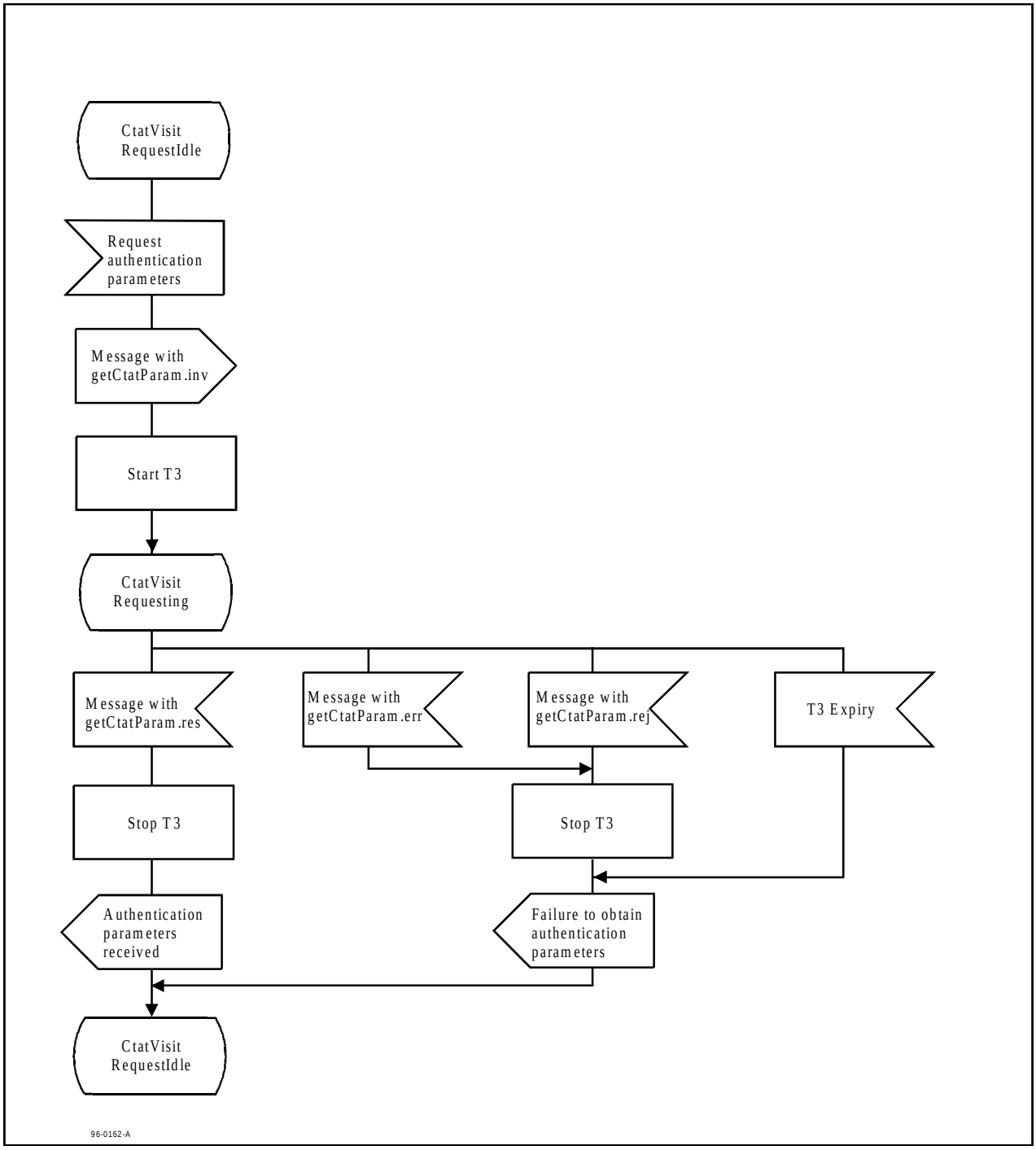

Figure C.5 - SDL representation of SS-CTAT at the Visitor PINX for requesting authentication parameters

C.6 SDL representation of SS-CTAT at the Authentication Server PINX

Figure C.6 shows the behaviour of an SS-CTAT Supplementary Service Control entity within the Authentication Server PINX.

Input signals from the right and output signals to the right represent primitives to and from the Coordination Function in respect of messages received from and sent to the Home PINX. Also protocol timer expiry is indicated by an input signal from the right.

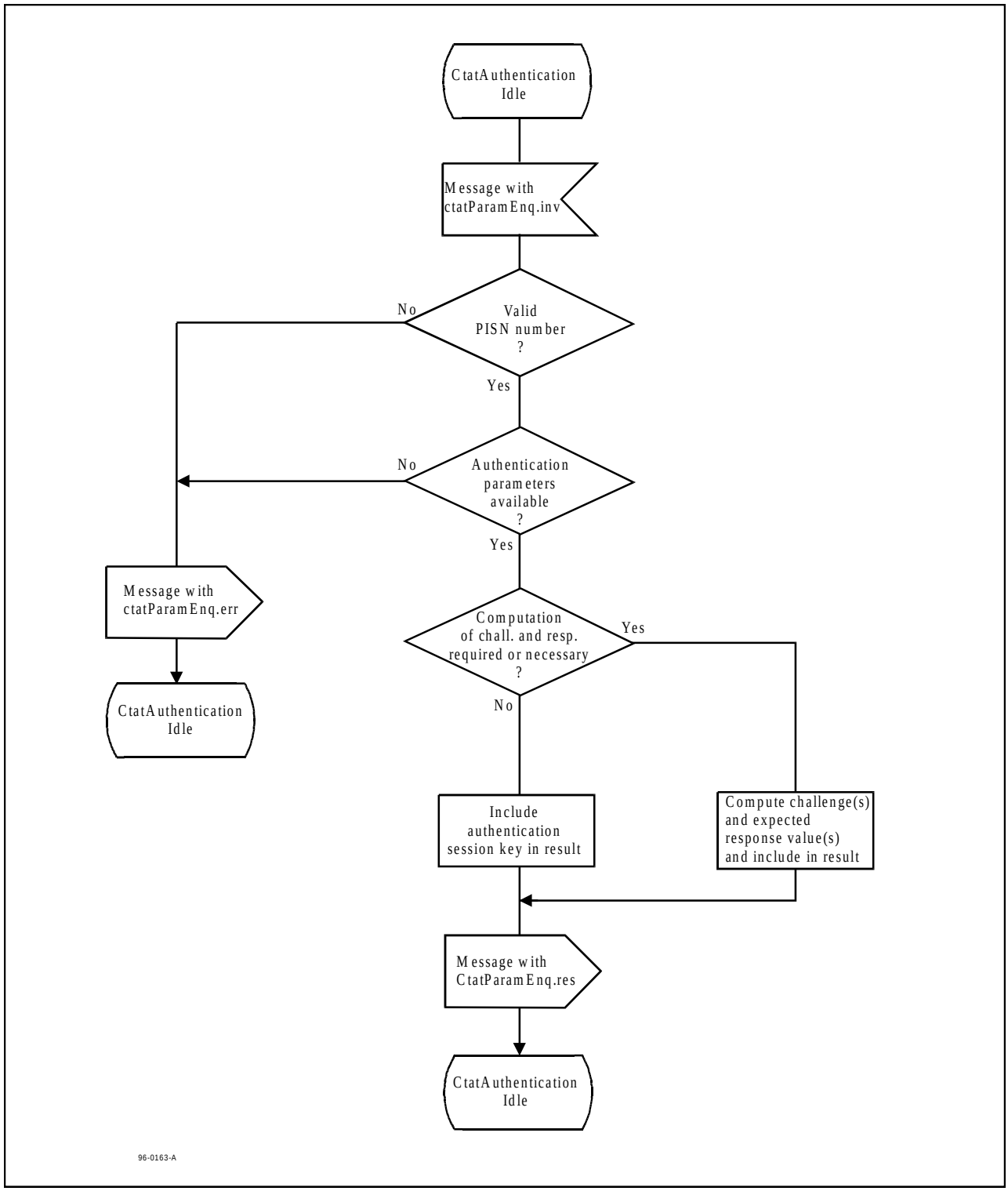

Figure C.6 - SDL representation of SS-CTAT at the Authentication Server PINX

C.7 SDL representation of SS-CTAN at the Visitor PINX

Figure C.7 shows the behaviour of an SS-CTAN Supplementary Service Control entity within the Visitor PINX.

Input signals from the left and output signals to the left represent primitives to and from the CTM user.

Input signals from the right and output signals to the right represent primitives to and from the Coordination Function in respect of messages received from and sent to the Home PINX. Also protocol timer expiry is indicated by an input signal from the right.

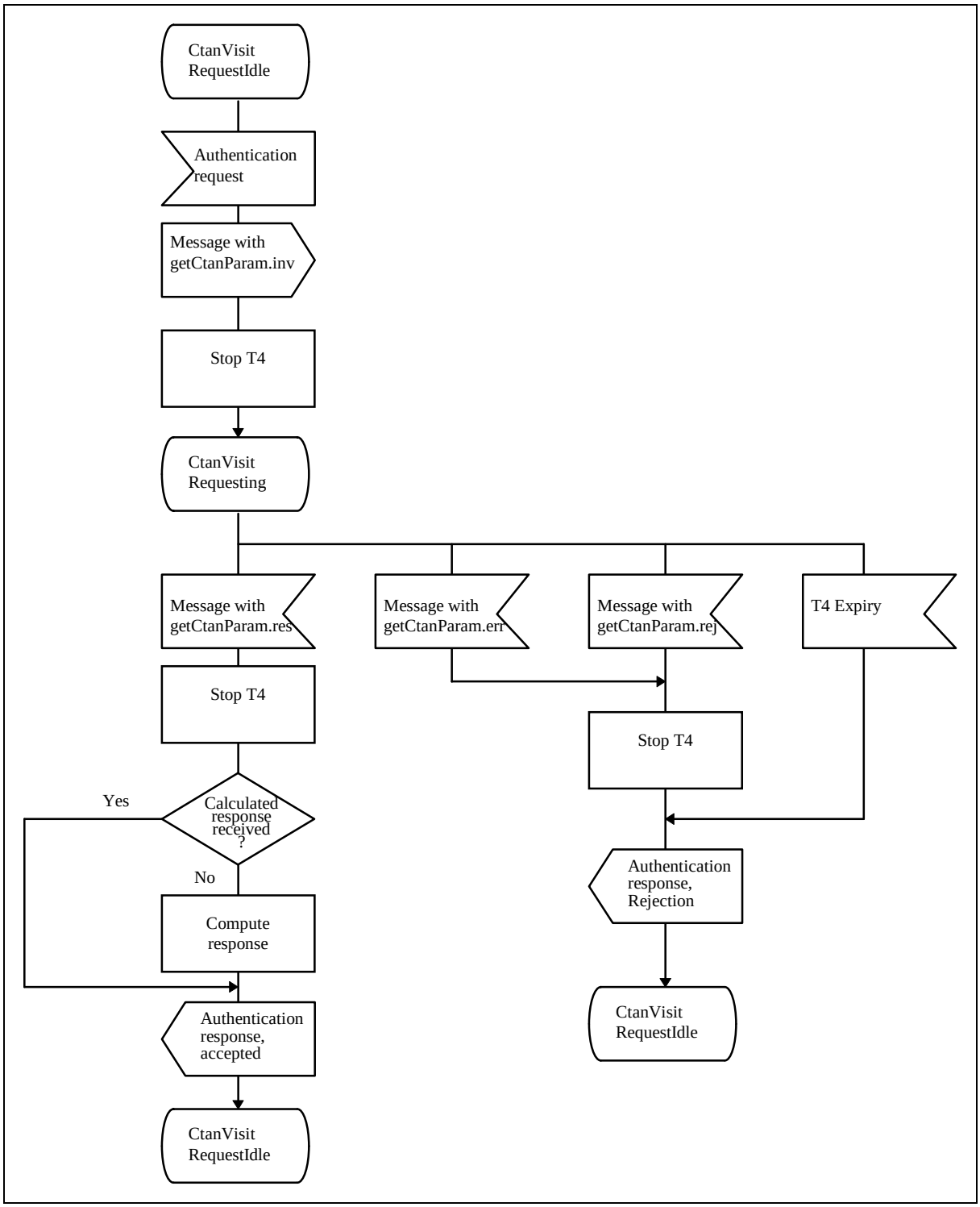

Figure C.7 - SDL representation of SS-CTAN at the Visitor PINX

C.8 SDL representation of SS-CTAN at the Home PINX

Figure C.8 shows the behaviour of an SS-CTAN Supplementary Service Control entity within the Home PINX.

Input signals from the right and output signals to the right represent primitives to and from the Coordination Function in respect of messages received and sent. Also protocol timer expiry is indicated by an input signal from the right.

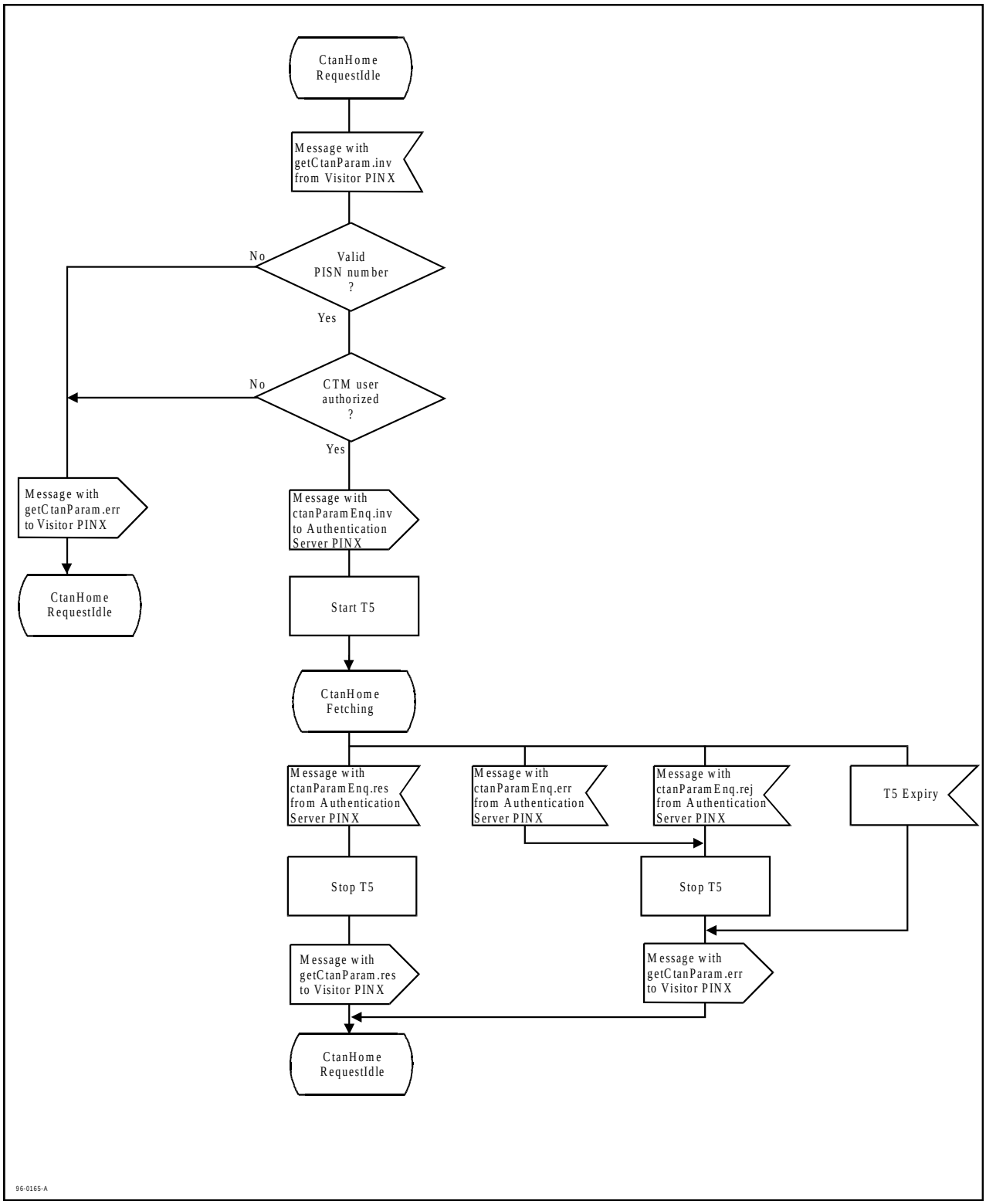

Figure C.8 - SDL representation of SS-CTAN at the Home PINX

C.9 SDL representation of SS-CTAN at the Authentication Server PINX

Figure C.9 shows the behaviour of an SS-CTAN Supplementary Service Control entity within the Authentication Server PINX.

Input signals from the right and output signals to the right represent primitives to and from the Coordination Function in respect of messages received from and sent to the Home PINX. Also protocol timer expiry is indicated by an input signal from the right.

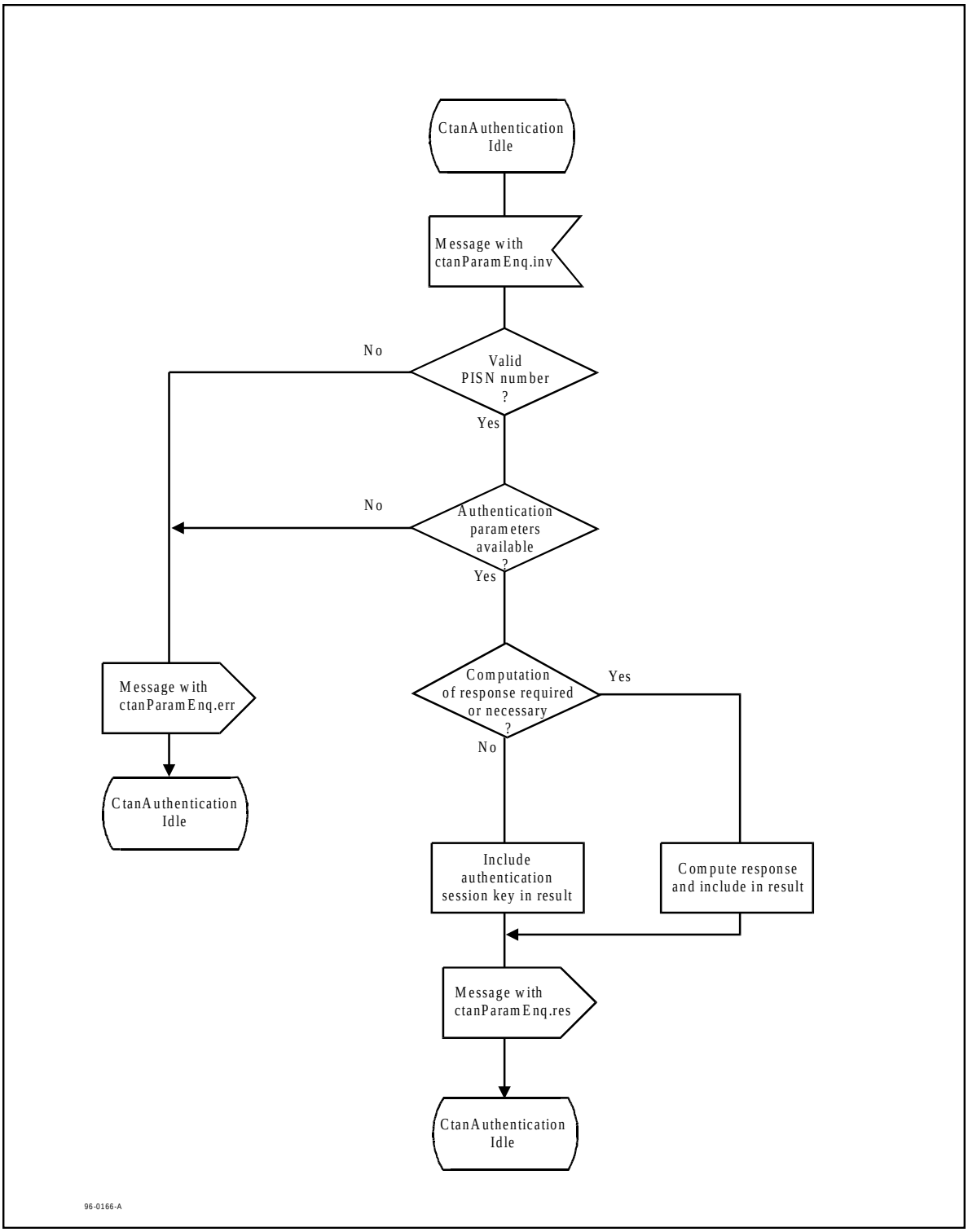

Figure C.9 - SDL representation of SS-CTAN at the Authentication Server PINX

Annex D

(informative)

Bibliography

I-ETS 300 768	Private Integrated Services Network (PISN); Cordless Terminal Mobility (CTM); Authentication; Service description (1993)
I-ETS 300 769	Private Integrated Services Network (PISN); Cordless Terminal Mobility (CTM); Authentication; Functional capabilities and information flows (1993)

Annex E

(informative)

Imported ASN.1 definitions

Table E.1 is an extract from module General-Error-List in ITU-T Rec. Q.950.

Table E.1 - Imported ASN.1 definitions General-Error-List

invalidServedUserNr ERROR ::= 6 -- The served users number provided is not a valid number.

Table E.2 is an extract from module Addressing-Data-Elements in ISO/IEC 11582.

Table E.2 - Imported ASN.1 definitions Addressing-Data-Elements

```
PartyNumber ::=  CHOICE {
                    unknownPartyNumber          [0] IMPLICIT NumberDigits,
                    -- the numbering plan is the default numbering plan of the network.
                    -- It is recommended that this value is used.
                    publicPartyNumber           [1] IMPLICIT PublicPartyNumber,
                    -- the numbering plan is according to Recs. E.163 and E.164.
                    dataPartyNumber             [3] IMPLICIT NumberDigits,
                    -- not used, value reserved.
                    telexPartyNumber            [4] IMPLICIT NumberDigits,
                    -- not used, value reserved.
                    privatePartyNumber          [5] IMPLICIT PrivatePartyNumber,
                    nationalStandardPartyNumber [8] IMPLICIT NumberDigits}
                    -- not used, value reserved.
PublicPartyNumber ::=  SEQUENCE {
                           publicTypeOfNumber       PublicTypeOfNumber,
                           publicNumberDigits       NumberDigits }
PrivatePartyNumber ::= SEQUENCE {
                           privateTypeOfNumber      PrivateTypeOfNumber,
                           privateNumberDigits      NumberDigits}
NumberDigits ::=       NumericString (SIZE(1..20))
PublicTypeOfNumber ::= ENUMERATED {
                           unknown                  (0),
                           -- if used number digits carry prefix indicating type of number
                           -- according to national recommendations
                           internationalNumber      (1),
                           nationalNumber           (2),
                           networkSpecificNumber    (3),
                           -- not used, value reserved.
                           subscriberNumber         (4),
                           abbreviatedNumber        (6)}
                           -- valid only for called party number at the outgoing access,
                           -- network substitutes appropriate number
PrivateTypeOfNumber ::= ENUMERATED {
                            unknown                 (0),
                            level2RegionalNumber    (1),
                            level1RegionalNumber    (2),
                            pISNSpecificNumber      (3),
                            localNumber             (4),
                            abbreviatedNumber       (6)}
```

Printed copies can be ordered from:

ECMA
114 Rue du Rhône
CH-1204 Geneva
Switzerland

Fax: +41 22 849.60.01
Internet: documents@ecma.ch

Files can be downloaded from our FTP site, **ftp.ecma.ch,** logging in as **anonymous** and giving your E-mail address as **password**. This Standard is available from library **ECMA-ST** as a compacted, self-expanding file in MSWord 6.0 format (file E243-DOC.EXE) and as an Acrobat PDF file (file E243-PDF.PDF). File E243-EXP.TXT gives a short presentation of the Standard.

Our web site, http://www.ecma.ch, gives full information on ECMA, ECMA activities, ECMA Standards and Technical Reports.

ECMA

114 Rue du Rhône
CH-1204 Geneva
Switzerland

This Standard ECMA-243 is available free of charge in printed form and as a file.

See inside cover page for instructions