INTERNATIONAL STANDARD

ISO/IEC 15433

Second edition
2003-04-01

Information technology — Telecommunications and information exchange between systems — Private Integrated Services Network — Inter-exchange signalling protocol — Wireless Terminal Authentication supplementary services

Technologies de l'information — Télécommunications et échange d'information entre systèmes — Réseau privé à intégration de services — Protocole de signalement d'interéchange — Services supplémentaires d'authentification de terminal sans fil

Reference number
ISO/IEC 15433:2003(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Annexes

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 15433 was prepared by ECMA (as ECMA-306) and was adopted, under a special "fast-track procedure", by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

This second edition cancels and replaces the first edition (ISO/IEC 15433:1999), which has been technically revised.

Introduction

This International Standard is one of a series of Standards defining Wireless Terminal Mobility (WTM) 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.

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

This International 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 JTC 1, ITU-T, ETSI and other international and national standardization bodies. It represents a pragmatic and widely based consensus.

Information technology — Telecommunications and information exchange between systems — Private Integrated Services Network — Inter-exchange signalling protocol — Wireless Terminal Authentication supplementary services

1 Scope

This International Standard specifies the signalling protocol for the support of the Wireless Terminal Authentication supplementary services (SS-WTAT and SS-WTAN) at the Q reference point between Private Integrated services Network eXchanges (PINXs) connected together within a Private Integrated Services Network (PISN).

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

Authentication of the PISN (SS-WTAN) is a supplementary service that enables a served WTM 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 International 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 ITU-T Rec. I.130. This International 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 ISO/IEC 15432.

The signalling protocol for SS-WTAT and SS-WTAN uses certain aspects of the generic procedures for the control of supplementary services specified in ISO/IEC 11582.

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

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

2 Conformance

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

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 11571:1998, *Information technology - Telecommunications and information exchange between systems - Private Integrated Services Networks - Addressing*

ISO/IEC 11574:2000, *Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Circuit-mode 64 kbit/s bearer services - Service description, functional capabilities and information flows*

ISO/IEC 11579-1:1994, *Information technology - Telecommunications and information exchange between systems - Private integrated services network - Part 1: Reference configuration for PISN Exchanges (PINX)*

ISO/IEC 11582:2002, *Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Generic functional protocol for the support of supplementary services - Inter-exchange signalling procedures and protocol*

ISO/IEC 15428:1999, *Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Specification, functional model and information flows - Wireless Terminal Location Registration supplementary service and Wireless Terminal Information Exchange additional network feature*

ISO/IEC 15429:2003, *Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Inter-exchange signalling protocol - Wireless Terminal Location Registration supplementary service and Wireless Terminal Information exchange additional network feature*

ISO/IEC 15432:1999, *Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Specification, functional model and information flows - Wireless Terminal Authentication supplementary services (WTAT and WTAN)*

ITU-T Rec. I.112:1993, *Vocabulary of terms for ISDNs*

ITU-T Rec. I.130:1988, *Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN (Blue Book)*

ITU-T Rec. I.210:1993, *Principles of telecommunication services supported by an ISDN and the means to describe them*

ITU-T Rec. Q.950:2000, *Supplementary services protocols, structure and general principles*

ITU-T Rec. Z.100:1999, *Specification and description language (SDL)*

4 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

4.1 External definitions

This International Standard uses the following terms defined in other documents:

– Application Protocol Data Unit (APDU)	(ISO/IEC 11582)
– Coordination Function	(ISO/IEC 11582)
– End PINX	(ISO/IEC 11582)
– Home Data Base (HDB)	(ISO/IEC 15428)
– Home PINX	(ISO/IEC 15428)
– Interpretation APDU	(ISO/IEC 11582)
– Network Facility Extension (NFE)	(ISO/IEC 11582)
– Originating PINX	(ISO/IEC 11582)
– PISN Number	(ISO/IEC 11571)
– Private Integrated Services Network (PISN)	(ISO/IEC 11579-1)
– Private Integrated services Network eXchange (PINX)	(ISO/IEC 11579-1)
– Signalling	(ITU-T Rec. I.112)
– Supplementary Service	(ITU-T Rec. I.210)
– Supplementary Services Control Entity	(ISO/IEC 11582)
– Terminating PINX	(ISO/IEC 11582)
– Transit PINX	(ISO/IEC 11582)
– User	(ISO/IEC 11574)
– Visitor area	(ISO/IEC 15428)
– Visitor PINX	(ISO/IEC 15428)
– WTM user	(ISO/IEC 15432)
– WTM user’s identity	(ISO/IEC 15428)

4.2 Other definitions

4.2.1 Authentication Server PINX

The PINX that contains the functionality to compute a challenge for a WTM user.

5 Symbols and abbreviated terms

ANF	Additional Network Feature
APDU	Application Protocol Data Unit
ASN.1	Abstract Syntax Notation no. 1
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-WTAN	Supplementary service - Authentication of a PISN
SS-WTAT	Supplementary service - Authentication of a WTM user
WT	Wireless Terminal
WTM	Wireless Terminal Mobility

6 Signalling protocol for the support of SS-WTAT

6.1 SS-WTAT description

SS-WTAT is a supplementary service which enables the PISN, as a security measure, to validate the identity provided by the WTM user. This is done by sending specific information to the WTM user and awaiting a response. If the received response is the expected response then authentication has passed successfully.

6.2 SS-WTAT operational requirements

6.2.1 Requirements on a Visitor PINX

Generic procedures for the call-independent control (connection-oriented) of supplementary services, as specified in ISO/IEC 11582 for an Originating and Terminating PINX, shall apply.

6.2.2 Requirements on a Home PINX

Generic procedures for the call-independent control (connection-oriented) of supplementary services, as specified in ISO/IEC 11582 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 ISO/IEC 11582 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 ISO/IEC 11582 for a Transit PINX, shall apply.

6.3 SS-WTAT coding requirements

6.3.1 Operations

The operations defined in Abstract Syntax Notation number 1 (ASN.1) in table 1 shall apply. The notation is in accordance with ITU-T Rec. X.680 and X.690. The ITU-T Rec. X.208 and X.209 superseded version is in annex E.

Table 1 - Operations in support of Authentication services

```
WTM-Authentication–Operations-asn1-97
                    {iso standard pss1-authentication (15433) authentication–operations-asn1-97 (1)}

DEFINITIONS EXPLICIT TAGS ::=

BEGIN

IMPORTS             OPERATION, ERROR FROM Remote-Operations-Information-Objects
                         {joint-iso-itu-t(2) remote-operations(4) informationObjects(5) version1(0)}
                    EXTENSION, Extension{} FROM Manufacturer-specific-service-extension-class-asn1-97
                         {iso standard
                         pss1-generic-procedures (11582) msi-class-asn1-97 (11)}
                    invalidServedUserNr FROM General-Error-List
                         {ccitt recommendation q 950 general-error-list (1)}
                    PartyNumber FROM Addressing-Data-Elements-asn1-97
                         {iso(1) standard(0) pss1-generic-procedures(11582)
                         addressing-data-elements-asn1-97(20)};

WTMAuth-Operations OPERATION ::= {authWtmUser | getWtatParam | wtatParamEnq | getWtanParam |
                              wtanParamEnq | transferAuthParam}

-- The following three operations shall apply to SS-WTAT --

authWtmUser         OPERATION ::= {  -- from Home PINX to Visitor PINX--
                    ARGUMENT         AuthWtmArg
                    RESULT           AuthWtmRes
                    ERRORS           { temporarilyUnavailable | invalidServedUserNr |
                                       notAuthorized | paramNotAvailable | unspecified}
                    CODE             local : 72}

getWtatParam        OPERATION ::= {  -- from Visitor PINX to Home PINX --
                    ARGUMENT         WtatParamArg
                    RESULT           WtatParamRes
                    ERRORS           { invalidServedUserNr | notAuthorized |
                                       paramNotAvailable | temporarilyUnavailable | unspecified}
                    CODE             local : 73}

wtatParamEnq        OPERATION ::= {  -- from Home PINX to Authentication Server PINX--
                    ARGUMENT         WtatParamArg
                    RESULT           WtatParamRes
                    ERRORS           { invalidServedUserNr | paramNotAvailable | unspecified}
                    CODE             local : 74}

AuthWtmArg ::=      SEQUENCE         {
                                     wtmUserId         WtmUserId,
                                     calcWtatInfo      [ 1 ] IMPLICIT CalcWtatInfo OPTIONAL,
                                     dummyExtension    DummyExtension OPTIONAL}
```

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

```
AuthWtmRes ::=          SEQUENCE        {
                                        autWtmResValue  ENUMERATED
                                                                {auth-res-correct (0),
                                                                auth-res-incorrect (1) },
                                        dummyExtension  DummyExtension OPTIONAL}

WtatParamArg ::=        SEQUENCE        {
                                        wtmUserId       WtmUserId,
                                        canCompute      CanCompute OPTIONAL,
                                        authChallenge   AuthChallenge 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 --

WtatParamRes ::=        SEQUENCE        {wtatParamInfo  WtatParamInfo,
                                        dummyExtension  DummyExtension OPTIONAL}

-- The following two operations shall apply to SS-WTAN --

getWtanParam            OPERATION ::= {  -- from Visitor PINX to Home PINX --
                        ARGUMENT        WtanParamArg
                        RESULT          WtanParamRes
                        ERRORS          { invalidServedUserNr | notAuthorized |
                                          paramNotAvailable | temporarilyUnavailable | unspecified}
                        CODE            local : 75}

wtanParamEnq            OPERATION ::= { -- from Home PINX to Authentication Server PINX--
                        ARGUMENT        WtanParamArg
                        RESULT          WtanParamRes
                        ERRORS          { invalidServedUserNr | paramNotAvailable | unspecified}
                        CODE            local : 76}

WtanParamArg ::=        SEQUENCE        { wtmUserId     WtmUserId,
                                        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 --

WtmUserId ::=           CHOICE    { pisnNumber      PartyNumber,
                                        -- The PISN number of the WTM user,
                                        -- always a Complete Number.
                                   alternativeId    AlternativeId }

AlternativeId ::=       OCTET STRING(SIZE(1..20))

WtanParamRes ::=        SEQUENCE        {wtanParamInfo  WtanParamInfo,
                                        dummyExtension  DummyExtension OPTIONAL}
```

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

```
-- The following unconfirmed operation shall apply when interaction between SS-WTAT and ANF-WTINFO --

transferAuthParam       OPERATION ::= {  -- from Home PINX to Visitor PINX --
                        ARGUMENT                SEQUENCE {
                                                        wtatParamInfo           WtatParamInfo,
                                                        dummyExtension          DummyExtension OPTIONAL}
                        RETURN RESULT           FALSE
                        ALWAYS RESPONDS         FALSE
                        CODE                    local : 77}

WtatParamInfo ::=       SEQUENCE        {authAlgorithm                  AuthAlgorithm,
                                        wtatParamInfoChoice             CHOICE {
                                                authSessionKeyInfo      [ 1 ] IMPLICIT AuthSessionKeyInfo,
                                                calcWtatInfo            [ 2 ] IMPLICIT CalcWtatInfo,
                                                authKey                 [ 3 ] IMPLICIT AuthKey,
                                                challLen                [ 4 ] IMPLICIT INTEGER(1..8) } }

AuthKey ::=             OCTET STRING (SIZE(1..16))   -- Authentication key --

WtanParamInfo ::=       CHOICE    {authSessionKeyInfo      [ 1 ] IMPLICIT AuthSessionKeyInfo,
                                  calcWtanInfo             [ 2 ] IMPLICIT CalcWtanInfo}

AuthSessionKeyInfo ::=  SEQUENCE        {authSessionKey    AuthSessionKey,
                                        calculationParam   CalculationParam}

CalcWtatInfo ::=        SEQUENCE SIZE(1..5) OF CalcWtatInfoUnit

CalcWtatInfoUnit ::=    SEQUENCE        {authChallenge     AuthChallenge,
                                        authResponse       AuthResponse,
                                        derivedCipherKey   [1] IMPLICIT DerivedCipherKey OPTIONAL,
                                        calculationParam   [2] IMPLICIT CalculationParam OPTIONAL}
                                        -- included if required by the authentication algorithm in use --

CalcWtanInfo ::=        SEQUENCE        {authResponse      AuthResponse,
                                        calculationParam   CalculationParam OPTIONAL}
                                        -- included if required by the authentication algorithm in use --

DummyExtension ::=      CHOICE    {extension         [5] IMPLICIT Extension{{WTMAuthExtSet}},
                                  sequOfExtn         [6] IMPLICIT SEQUENCE OF
                                                                 Extension{{WTMAuthExtSet}} }

AUTH-ALG                ::= CLASS  {
                        &id DefinedIDs UNIQUE,
                        &Type OPTIONAL
                                  }

DefinedIDs ::= INTEGER { ct2 (0), dect (1), gsm (2), pci (3), pwt (4), us-gsm (5), phs (6), tetra (7) } (0..255)

AuthAlgSet AUTH-ALG ::= {...}

AuthAlgorithm ::=    SEQUENCE     {
                        authAlg   AUTH-ALG.&id({AuthAlgSet}),
                        param     AUTH-ALG.&Type({AuthAlgSet}{@.authAlg}) OPTIONAL
                                  }

AuthChallenge ::=       OCTET STRING (SIZE(1..8))    -- Randomly generated parameter --
```

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

```
AuthResponse ::=          OCTET STRING (SIZE(1..4))    -- WTAT: Expected response value --
                                                       -- WTAN: 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 WTM user during --
                                                       -- both WTAT and WTAN. --

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--

WTMAuthExtSet EXTENSION ::= {...}

notAuthorized             ERROR               ::=      {CODE local : 1007 }
paramNotAvailable         ERROR               ::=      {CODE local : 1017 }
temporarilyUnavailable    ERROR               ::=      {CODE local : 1000 }
unspecified               ERROR ::={
                                PARAMETER     Extension{{WTMAuthExtSet}}
                                CODE          local : 1008}

END                       -- of WTM-Authentication–Operations-asn1-97
```

6.3.2 Information elements

6.3.2.1 Facility information element

APDUs of the operations defined in 6.3.1 shall be coded in the Facility information element in accordance with ISO/IEC 11582.

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

When conveying the invoke APDUs 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 ISO/IEC 11582.

6.3.3 Messages

The Facility information element shall be conveyed in the messages as specified in clause 10 of ISO/IEC 11582.

6.4 SS-WTAT state definitions

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

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

6.4.1.1 State WtatHomeInitIdle

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

6.4.1.2 State WtatHomeInitiating

An authWtmUser 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-WTAT Supplementary Service Control entity in that PINX in association with a particular request for authentication of a WTM user.

6.4.2.1 State WtatHomeRequestIdle

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

6.4.2.2 State WtatHomeRequesting

A getWtatParam 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-WTAT Supplementary Service Control entity in that PINX in association with a particular request for authentication of a WTM user.

6.4.3.1 State WtatHomeFetchIdle

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

6.4.3.2 State WtatHomeFetching

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

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

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

6.4.4.1 State WtatVisitExecIdle

Execution of SS-WTAT is not in progress.

6.4.4.2 State WtatVisitExecuting

An authWtmUser invoke APDU has been received from the Home PINX and execution of SS-WTAT 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-WTAT Supplementary Service Control entity in that PINX in association with a particular request for authentication of a WTM user.

6.4.5.1 State WtatVisitRequestIdle

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

6.4.5.2 State WtatVisitRequesting

A getWtatParam 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-WTAT Supplementary Service Control entity in that PINX in association with a particular request for authentication of a WTM user.

6.4.6.1 State WtatAuthenticationIdle

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

6.5 SS-WTAT Signalling procedures

Examples of message sequences are shown in annex C.

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

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

6.5.1.1 Normal procedures

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

On determining that the SS-WTAT 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 authWtmUser invoke APDU to the Visitor PINX containing the element calcWtatInfo.

The authWtmUser 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 ISO/IEC 11582. The Home PINX shall enter state WtatHomeInitiating and start timer T1.

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

NOTE 1 - Confirmation of the authentication of the WTM 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 authWtmUser return error or reject APDU from the Visitor PINX, the Home PINX shall stop timer T1 and enter state WtatHomeInitIdle.

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

NOTE 2 - Failure of the authentication of the WTM 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 D.2 of annex D.

6.5.2.1 Normal procedures

On receipt of a getWtatParam invoke APDU using the call reference of a call-independent signalling connection (as specified in 7.3 of ISO/IEC 11582), the Home PINX shall check that the received WTM user’s identity is valid and that the WTM user is authorized for SS-WTAT. The Home PINX shall then enter state WtatHomeRequesting 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 getWtatParam invoke APDU with a return result APDU containing the authentication parameters received from the Authentication Server PINX. The Home PINX shall enter state WtatHomeRequestIdle.

6.5.2.2 Exceptional procedures

If the received WTM user’s identity is not valid, the Home PINX shall answer the getWtatParam invoke APDU with a return error APDU containing the error invalidServedUserNr and remain in state WtatHomeRequestIdle.

If the WTM user is not authorized for SS-WTAT, the Home PINX shall answer the getWtatParam invoke APDU with a return error APDU containing the error notAuthorized and remain in state WtatHomeRequestIdle.

If authentication parameters are not received for any reason during the procedures of 6.5.3, the Home PINX shall answer the getWtatParam invoke APDU with a return error APDU and enter state WtatHomeRequestIdle. 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 D.3 of annex D.

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 wtatParamEnq 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 getWtatParam invoke APDU) that it is able to compute its own challenge and response. Element authChallenge shall be included if it was provided by the Visitor PINX. 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 ISO/IEC 11582. The Home PINX shall enter state WtatHomeFetching and start timer T2.

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

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 wtatParamEnq return error or reject APDU from the Authentication Server PINX, the Home PINX shall stop timer T2 and enter state WtatHomeFetchIdle.

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

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-WTAT

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

6.5.4.1 Normal procedures

On determining that SS-WTAT is to be invoked and when the authentication parameters are not available in the Visitor PINX for this WTM 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. Element authChallenge may be included if the Visitor PINX is capable of calculating a challenge. 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, SS-WTAT shall be executed.

6.5.4.2 Exceptional procedures

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

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

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

6.5.5.1 Normal procedures

On receipt of an authWtmUser invoke APDU using the call reference of a call-independent signalling connection (as specified in 7.3 of ISO/IEC 11582) and when either element calcWtatInfo is included or authentication parameters for this WTM user are already available at the Visitor PINX, a request for authentication shall be sent to the WTM user and the Visitor PINX shall enter state WtatVisitExecuting.

If the element calcWtatInfo is not included in the authWtmUser invoke APDU and when the authentication parameters for this WTM user are not available at the Visitor PINX, the Visitor PINX shall enter state WtatVisitExecuting. 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. Element authChallenge may be included if the Visitor PINX is capable of calculating a challenge. 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 WTM user.

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

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 authWtmUser invoke APDU with a return error APDU and enter state WtatVisitExecIdle.

If the authentication request is not answered by the WTM user, the Visitor PINX shall answer the authWtmUser invoke APDU with a return error APDU containing the error temporarilyUnavailable and enter state WtatVisitExecIdle.

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 D.5 of annex D.

6.5.6.1 Normal procedures

In order to make an enquiry to the Home PINX to request the authentication parameters for a WTM user, the Visitor PINX shall send a getWtatParam 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 ISO/IEC 11582. The Visitor PINX shall start timer T3 and enter state WtatVisitRequesting.

On receipt of the getWtatParam return result APDU, the Visitor PINX shall stop timer T3 and enter state WtatVisitRequestIdle. If the element wtatParamInfo contains authentication session key, the Visitor PINX shall calculate the challenge and the expected response. If the element wtatParamInfo contains calcWtatInfo no calculation is necessary.

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 getWtatParam return error or reject APDU from the Home PINX, the Visitor PINX shall stop timer T3 and enter state WtatVisitRequestIdle.

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

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 D.6 of annex D.

6.5.7.1 Normal procedures

On receipt of a wtatParamEnq invoke APDU using the call reference of a call-independent signalling connection (as specified in 7.3 of ISO/IEC 11582), the Authentication Server PINX shall check that the received WTM user’s identity is valid and retrieve the authentication parameters if available.

Further processing depends on the application:

- If it is required by the application or if the element canCompute is not included in the wtatParamEnq invoke APDU, the Authentication Server PINX shall generate challenge(s) unless one is provided, and use the authentication keys to compute the expected response value(s), and answer the wtatParamEnq invoke APDU with a return result APDU where element wtatParamInfo contains the calculated authentication information (choice calcWtatInfo).
- If the element canCompute is included in the wtatParamEnq 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 wtatParamEnq invoke APDU with a return result APDU where element wtatParamInfo contains the authentication session key (choice authSessionKeyInfo).
- Choices authKey and challLen shall not be used in the wtatParamEnq return result APDU.

The wtatParamEnq return result APDU shall contain the authentication algorithm in use. The Authentication Server PINX shall remain in state WtatAuthenticationIdle.

6.5.7.2 Exceptional procedures

If the received WTM user’s identity is not valid, the Authentication Server PINX shall answer the wtatParamEnq invoke APDU with a return error APDU containing the error invalidServedUserNr and remain in state WtatAuthenticationIdle.

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

6.5.8 Actions at a Transit PINX

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

6.6 SS-WTAT Impact of interworking with public ISDNs

Not applicable.

6.7 SS-WTAT Impact of interworking with non-ISDNs

Not applicable.

6.8 Protocol interactions between SS-WTAT 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 International Standard. For interactions with supplementary services and ANFs for which stage 3 Standards are published subsequent to the publication of this International Standard, see those other stage 3 Standards.

NOTE 3 - Additional interactions that have no impact on the signalling protocol at the Q reference point can be found in the relevant stage 1 specifications.

NOTE 4 - Simultaneous conveyance of APDUs for SS-WTAT 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 Calling Name Identification Presentation (SS-CNIP)

No protocol interaction.

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

No protocol interaction.

6.8.3 Interaction with Completion of Calls to Busy Subscriber (SS-CCBS)

No protocol interaction.

6.8.4 Interaction with Completion of Calls on No Reply (SS-CCNR)

No protocol interaction.

6.8.5 Interaction with Call Transfer (SS-CT)

No protocol interaction.

6.8.6 Interaction with Call Forwarding Unconditional (SS-CFU)

No protocol interaction.

6.8.7 Interaction with Call Forwarding Busy (SS-CFB)

No protocol interaction.

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

No protocol interaction.

6.8.9 Interaction with Call Deflection (SS-CD)

No protocol interaction.

6.8.10 Interaction with Path Replacement (ANF-PR)

No protocol interaction.

6.8.11 Interaction with Call Offer (SS-CO)

No protocol interaction.

6.8.12 Interaction with Call Intrusion (SS-CI)

No protocol interaction.

6.8.13 Interaction with Do Not Disturb (SS-DND)

No protocol interaction.

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

No protocol interaction.

6.8.15 Interaction with Advice Of Charge (SS-AOC)

No protocol interaction.

6.8.16 Interaction with Recall (SS-RE)

No protocol interaction.

6.8.17 Interaction with Call Interception (ANF-CINT)

No protocol interaction.

6.8.18 Interaction with Transit Counter (ANF-TC)

No protocol interaction.

6.8.19 Interaction with Route Restriction Class (ANF-RRC)

No protocol interaction.

6.8.20 Interaction with Message Waiting Information (SS-MWI)

No protocol interaction.

6.8.21 Interaction with Wireless Terminal Location Registration (SS-WTLR)

No protocol interaction.

6.8.22 Interaction with Wireless Terminal information exchange (ANF-WTINFO)

The following protocol interaction shall apply if ANF-WTINFO is supported in accordance with ISO/IEC 15429.

6.8.22.1 Actions at the Home PINX

On receipt of a getRRCInf invoke APDU the Home PINX may obtain authentication parameters and include a transferAuthParam invoke APDU in the same message as the getRRCInf return result APDU. The invoke APDU shall contain element wtatParamInfo with choice authKey or challLen.

6.8.22.2 Actions at the Visitor PINX

When the element wtatParamInfo 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 during authentication of the WTM user.

6.8.23 Interaction with Wireless Terminal Incoming Call (ANF-WTMI)

No protocol interaction.

6.8.24 Interaction with Wireless Terminal Outgoing Call (ANF-WTMO)

No protocol interaction.

6.8.25 Interaction with Authentication of the PISN (SS-WTAN)

No protocol interaction.

6.9 SS-WTAT parameter values (timers)

6.9.1 Timer T1

Timer T1 operates at the Home PINX during state WtatHomeInitiating. Its purpose is to protect against the absence of a response to the authWtmUser 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 WtatHomeFetching. Its purpose is to protect against the absence of a response to the wtatParamEnq 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 WtatVisitRequesting. Its purpose is to protect against the absence of a response to the getWtatParam invoke APDU.

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

7 Signalling protocol for the support of SS-WTAN

7.1 SS-WTAN description

SS-WTAN is a supplementary service which enables the WTM 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. If the received response is the expected response then authentication has passed successfully.

7.2 SS-WTAN 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 ISO/IEC 11582 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 ISO/IEC 11582 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 ISO/IEC 11582 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 ISO/IEC 11582 for a Transit PINX, shall apply.

7.3 SS-WTAN coding requirements

7.3.1 Operations

The operations getWtanParam and wtanParamEnq defined in the Abstract Syntax Notation number 1 (ASN.1) in table 1 in 6.3.1 shall apply to SS-WTAN.

7.3.2 Information elements

7.3.2.1 Facility information element

APDUs of the operations defined in 7.3.1 shall be coded in the Facility information element in accordance with ISO/IEC 11582.

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 rejectAnyUnrecognisedInvokePdu.

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 ISO/IEC 11582.

7.3.3 Messages

The Facility information element shall be conveyed in the messages as specified in clause 10 of ISO/IEC 11582.

7.4 SS-WTAN 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-WTAN Supplementary Service Control entity in that PINX in association with a particular request for authentication of a PISN.

7.4.1.1 State WtanVisitRequestIdle

SS-WTAN is not in progress.

7.4.1.2 State WtanVisitRequesting

A getWtanParam 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-WTAN Supplementary Service Control entity in that PINX in association with a particular request for authentication of a PISN.

7.4.2.1 State WtanHomeRequestIdle

Ready for receipt of a getWtanParam invoke APDU.

7.4.2.2 State WtanHomeFetching

A wtanParamEnq 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-WTAN Supplementary Service Control entity in that PINX in association with a particular request for authentication of a PISN.

7.4.3.1 State WtanAuthenticationIdle

Ready for receipt of a wtanParamEnq invoke APDU.

7.5 SS-WTAN 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 D.7 of annex D.

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

7.5.1.1 Normal procedures

On receipt of a valid authentication request from the WTM user and in order to make a request to the Home PINX to get the authentication parameters for this WTM user, the Visitor PINX shall send a getWtanParam invoke APDU to the Home PINX containing the challenge which was received from the WTM 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 getWtanParam 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 ISO/IEC 11582. The Visitor PINX shall enter state WtanVisitRequesting and start timer T4.

On receipt of the getWtanParam return result APDU, the Visitor PINX shall stop timer T4. The element wtanParamInfo contains either the authentication session key for the WTM user or the calculated response value. If it contains the authentication session key, the Visitor PINX shall use it and the challenge received from the WTM user to compute the response value for sending to the WTM 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 WTM user in acceptance of the authentication request. The Visitor PINX shall enter state WtanVisitRequestIdle.

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 getWtanParam return error or reject APDU from the Home PINX, the Visitor PINX shall stop timer T4. A response shall be sent to the WTM user indicating rejection of the authentication request, and the Visitor PINX shall enter state WtanVisitRequestIdle.

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

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 D.8 of annex D.

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 getWtanParam invoke APDU using the call reference of a call-independent signalling connection (as specified in 7.3 of ISO/IEC 11582), the Home PINX shall check that the received WTM user’s identity is valid and that the WTM user is authorized for the SS-WTAN. If authorized, the Home PINX shall then send a wtanParamEnq 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 ISO/IEC 11582. The Home PINX shall enter state WtanHomeFetching and start timer T5.

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

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 WTM user’s identity is not valid, the Home PINX shall answer the getWtanParam invoke APDU with a return error APDU containing the error invalidServedUserNr and remain in state WtanHomeRequestIdle.

If the WTM user is not authorized for SS-WTAN, the Home PINX shall answer the getWtanParam invoke APDU with a return error APDU containing the error notAuthorized and remain in state WtanHomeRequestIdle.

On receipt of a wtanParamEnq return error APDU from the Authentication Server PINX, the Home PINX shall stop timer T5 and answer the getWtanParam invoke APDU with the received error in a return error APDU and enter state WtanHomeRequestIdle.

On receipt of a wtanParamEnq reject APDU from the Authentication Server PINX, the Home PINX shall stop timer T5 and answer the getWtanParam invoke APDU with error paramNotAvailable in a return error APDU and enter state WtanHomeRequestIdle.

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

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 D.9 of annex D.

7.5.3.1 Normal procedures

On receipt of a wtanParamEnq invoke APDU using the call reference of a call-independent signalling connection (as specified in 7.3 of ISO/IEC 11582), the Authentication Server PINX shall check that the received WTM user's identity is valid and retrieve the authentication parameters if available.

Further processing depends on the application:

- If it is required by the application or if the element canCompute is not included in the wtanParamEnq invoke APDU, the Authentication Server PINX shall use the received challenge to compute a response value and answer the wtanParamEnq invoke APDU with a return result APDU where element wtanParamInfo contains the calculated response value (choice calcWtanInfo).
- If the element canCompute is included in the wtanParamEnq invoke APDU and if it is not required by the application to compute the expected response value, the Authentication Server PINX shall answer the wtanParamEnq invoke APDU with a return result APDU where element wtanParamInfo contains the authentication session key (choice authSessionKeyInfo).

The Authentication Server PINX shall remain in state WtanAuthenticationIdle.

7.5.3.2 Exceptional procedures

If the received WTM user's identity is not valid, the Authentication Server PINX shall answer the wtanParamEnq invoke APDU with a return error APDU containing the error invalidServedUserNr and remain in state WtanAuthenticationIdle.

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

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-WTAN impact of interworking with public ISDNs

Not applicable.

7.7 SS-WTAN impact of interworking with non-ISDNs

Not applicable.

7.8 Protocol interactions between SS-WTAN 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 International Standard. For interactions with supplementary services and ANFs for which stage 3 Standards are published subsequent to the publication of this International Standard, see those other stage 3 Standards.

NOTE 5 - Additional interactions that have no impact on the signalling protocol at the Q reference point can be found in the relevant stage 1 specifications.

NOTE 6 - Simultaneous conveyance of APDUs for SS-WTAN 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 Calling Name Identification Presentation (SS-CNIP)

No protocol interaction.

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

No protocol interaction.

7.8.3 Interaction with Completion of Calls to Busy Subscriber (SS-CCBS)

No protocol interaction.

7.8.4 Interaction with Completion of Calls on No Reply (SS-CCNR)

No protocol interaction.

7.8.5 Interaction with Call Transfer (SS-CT)

No protocol interaction.

7.8.6 Interaction with Call Forwarding Unconditional (SS-CFU)

No protocol interaction.

7.8.7 Interaction with Call Forwarding Busy (SS-CFB)

No protocol interaction.

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

No protocol interaction.

7.8.9 Interaction with Call Deflection (SS-CD)

No protocol interaction.

7.8.10 Interaction with Path Replacement (ANF-PR)

No protocol interaction.

7.8.11 Interaction with Call Offer (SS-CO)

No protocol interaction.

7.8.12 Interaction with Call Intrusion (SS-CI)

No protocol interaction.

7.8.13 Interaction with Do Not Disturb (SS-DND)

No protocol interaction.

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

No protocol interaction.

7.8.15 Interaction with Advice Of Charge (SS-AOC)

No protocol interaction.

7.8.16 Interaction with Recall (SS-RE)

No protocol interaction.

7.8.17 Interaction with Call Interception (ANF-CINT)

No protocol interaction.

7.8.18 Interaction with Transit Counter (ANF-TC)

No protocol interaction.

7.8.19 Interaction with Route Restriction Class (ANF-RRC)

No protocol interaction.

7.8.20 Interaction with Message Waiting Information (SS-MWI)

No protocol interaction.

7.8.21 Interaction with Wireless Terminal Location Registration (SS-WTLR)

No protocol interaction.

7.8.22 Interaction with Wireless Terminal information exchange (ANF-WTINFO)

No protocol interaction.

7.8.23 Interaction with Wireless Terminal Incoming Call (ANF-WTMI)

No protocol interaction.

7.8.24 Interaction with Wireless Terminal Outgoing Call (ANF-WTMO)

No protocol interaction.

7.8.25 Interaction with Authentication of the PISN (SS-WTAT)

No protocol interaction.

7.9 SS-WTAN parameter values (timers)

7.9.1 Timer T4

Timer T4 operates at the Visitor PINX during state WtanVisitRequesting. Its purpose is to protect against the absence of a response to the getWtanParam 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 WtanHomeFetching. Its purpose is to protect against the absence of a response to the wtanParamEnq 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 International 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 PICS's;
- 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 International 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 International 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-WTAT

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 suppliers 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 International Standard)

Date of statement	

A.3.3 General

Item	Question/feature	References	Status	N/A	Support
A1	Behaviour as Visitor PINX for SS-WTAT		o.1		Yes [ ] No [ ]
A2	Behaviour as Home PINX for SS-WTAT (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-WTAT (separate from a Home PINX)		o.1		Yes [ ] No [ ]

A.3.4 Procedures

Item	Question/feature	References	Status	N/A	Support
B1	Support of ISO/IEC 11582 procedures at a Visitor PINX	6.2.1	A1:m	[ ]	m: Yes [ ]
B2	Support of ISO/IEC 11582 procedures at a Home PINX	6.2.2	c.1	[ ]	m: Yes [ ]
B3	Support of ISO/IEC 11582 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-WTAT with challenge and expected response	6.5.5	A1:o	[ ]	Yes [ ] No [ ]
B5	Signalling procedures at a Visitor PINX for receiving request from Home PINX for SS-WTAT without challenge and expected response	6.5.5	A1:o	[ ]	Yes [ ] No [ ]
B6	Support of procedures for initiation of SS-WTAT at the Visitor PINX	6.5.4	A1:m	[ ]	m: Yes [ ]
B7	Signalling procedures at a Visitor PINX for requesting authentication parameters from Home PINX	6.5.6	A1:m	[ ]	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-WTAT without challenge and expected response	6.5.1	c.2	[ ]	Yes [ ] No [ ]
B10	Signalling procedures at a Home PINX for initiation of SS-WTAT with challenge and expected response	6.5.1	c.2	[ ]	Yes [ ] No [ ]
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 A2 or A3 then optional, else N/A

A.3.5 Coding

Item	Question/feature	References	Status	N/A	Support
C1	Sending of authWtmUser invoke APDU and receipt of return result and return error APDUs	6.3	c.3	[ ]	m: Yes [ ]
C2	Sending of getWtatParam invoke APDU and receipt of return result and return error APDUs	6.3	A1:m	[ ]	m: Yes [ ]
C3	Sending of wtatParamEnq invoke APDU and receipt of return result and return error APDUs	6.3	A2:m	[ ]	m: Yes [ ]
C4	Receipt of authWtmUser invoke APDU and sending of return result and return error APDUs	6.3	A1:o	[ ]	Yes [ ] No [ ]
C5	Receipt of getWtatParam invoke APDU and sending of return result and return error APDUs	6.3	B11:m	[ ]	m: Yes [ ]
C6	Receipt of wtatParamEnq invoke APDU and sending of return result and return error APDUs	6.3	A4:m	[ ]	m: Yes [ ]

c.3: if B9 or B10 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.4	[ ]	m: Yes [ ] Value [. . . .]
D2	Support of timer T2	6.9.2	A2:m	[ ]	m: Yes [ ] Value [. . . .]
D3	Support of timer T3	6.9.3	A1:m	[ ]	m: Yes [ ] Value [. . . .]

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

A.3.7 Protocol interactions with ANF-WTINFO

Item	Question/feature	Reference	Status	N/A	Support
E1	Support of ANF-WTINFO		o		Yes [ ] No [ ]
E2	Interactions at Home PINX	6.8.22.1	E1:o	[ ]	o: Yes [ ] No [ ]
E3	Interactions at Visitor PINX	6.8.22.2	E1:o	[ ]	o: Yes [ ] No [ ]

A.4 PICS proforma for SS-WTAN

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 suppliers 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 International Standard)

Date of statement	

A.4.3 General

Item	Question/feature	References	Status	N/A	Support
A1	Behaviour as Visitor PINX for SS-WTAN		o.1		Yes [ ] No [ ]
A2	Behaviour as Home PINX for SS-WTAN (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-WTAN (separate from a Home PINX)		o.1		Yes [ ] No [ ]

A.4.4 Procedures

Item	Question/feature	References	Status	N/A	Support
B1	Support of ISO/IEC 11582 procedures at a Visitor PINX	7.2.1	A1:m	[ ]	m: Yes [ ]
B2	Support of ISO/IEC 11582 procedures at a Home PINX	7.2.2	c.1	[ ]	m: Yes [ ]
B3	Support of ISO/IEC 11582 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 getWtanParam invoke APDU and receipt of return result and return error APDUs	7.3	A1:m	[ ]	m: Yes [ ]
C2	Sending of wtanParamEnq invoke APDU and receipt of return result and return error APDUs	7.3	A2:m	[ ]	m: Yes [ ]
C3	Receipt of getWtanParam invoke APDU and sending of return result and return error APDUs	7.3	c.2	[ ]	m: Yes [ ]
C4	Receipt of wtanParamEnq 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)

Imported ASN.1 definitions

The content of this annex has been deleted to remove duplicate ASN.1 definitions defined elsewhere.

Annex C
(informative)

Examples of message sequences

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

1. The following notation is used:

   - - - - - - - - ➤ Call-independent signalling connection message containing SS-WTAT/SS-WTAN information

   ---------------► Call-independent signalling connection message without SS-WTAT/SS-WTAN information

   ···············► Symbolic primitive carrying SS-WTAT/SS-WTAN 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-WTAT/SS-WTAN. Only messages relevant to SS-WTAT/SS-WTAN are shown.

3. Only the relevant information content (i.e. remote operation APDUs) is listed below each message name. The Facility information elements containing remote operation APDUs and notifications are not explicitly shown. Information with no impact on SS-WTAT/SS-WTAN 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 International Standard.

C.1 Successful authentication of a WTM user (SS-WTAT); the Visitor PINX initiates SS-WTAT

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

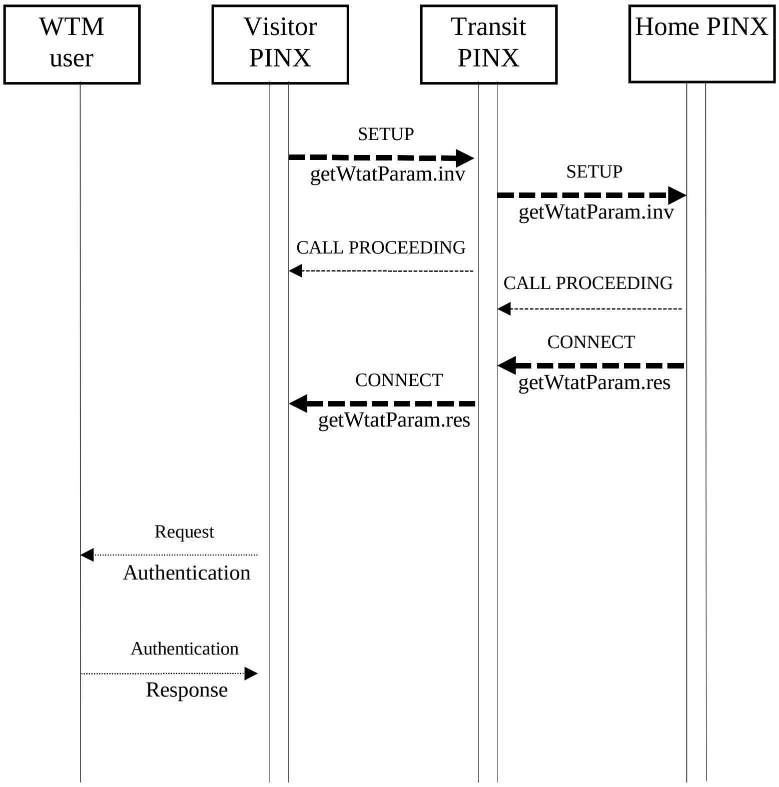

Figure C.1 - Example message flow for authentication of a WTM user

C.2 Successful authentication of a WTM user (SS-WTAT); the Home PINX initiates SS-WTAT without including challenge and response values

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

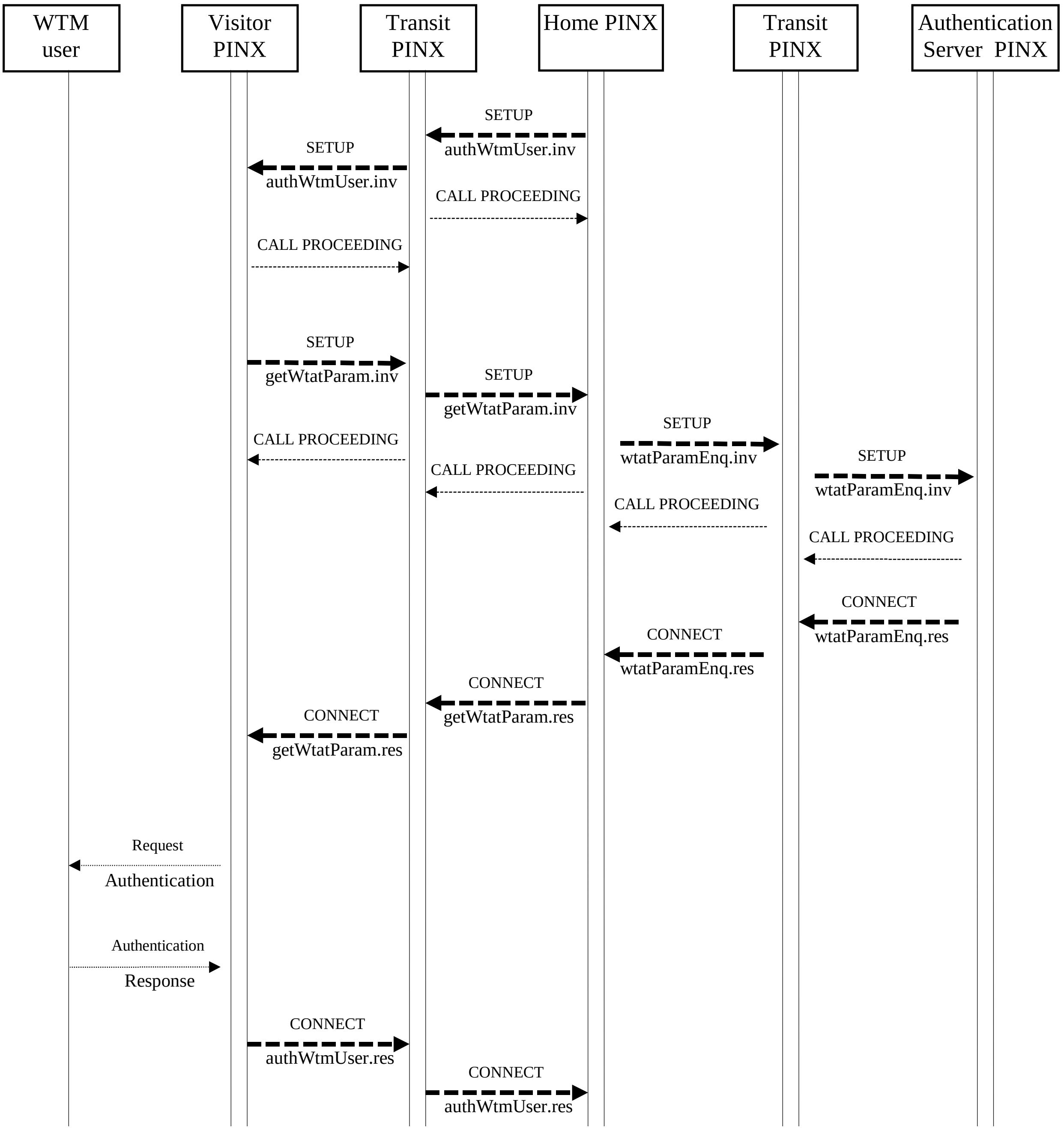

Figure C.2 - Example message flow for authentication of a WTM user

C.3 Successful authentication of a WTM user (SS-WTAT); the Home PINX initiates SS-WTAT with challenge and response values included

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

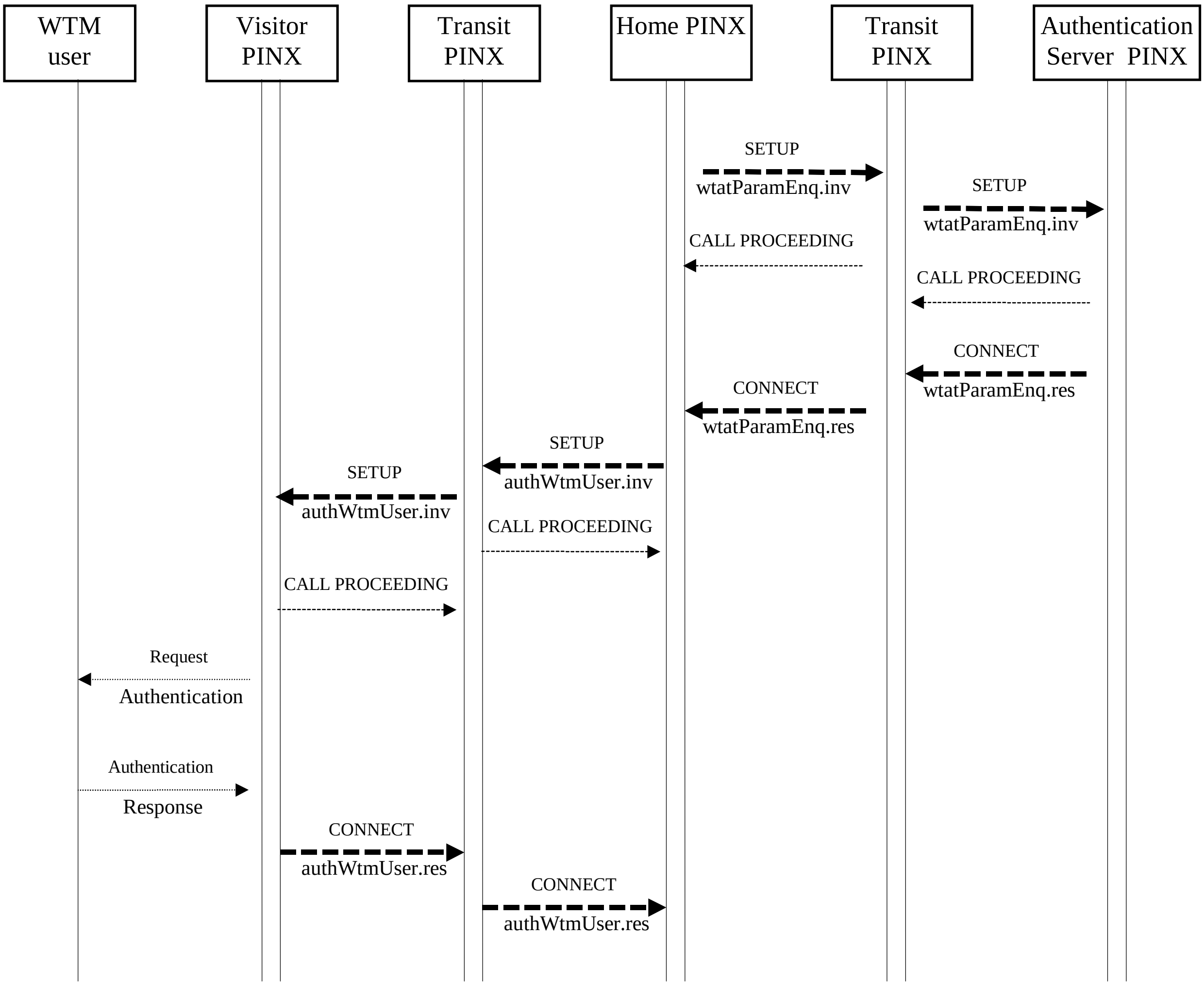

Figure C.3 - Example message flow for authentication of a WTM user

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

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

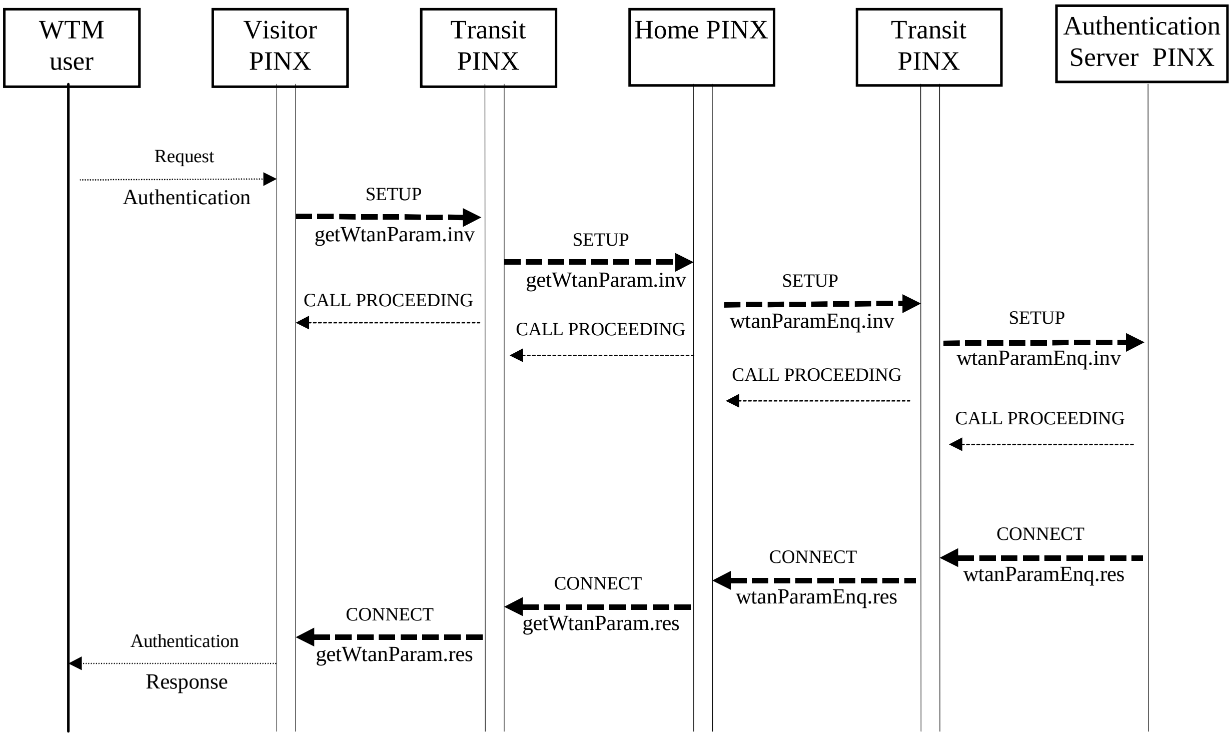

Figure C.4 - Example message flow for authentication of a PISN

Annex D
(informative)

Specification and Description Language (SDL) representation of procedures

The diagrams in this annex use the Specification and Description Language defined in ITU-T Recommendation Z.100.

Each diagram represents the behaviour of an SS-WTAT or SS-WTAN Supplementary Service Control entity at a particular type of PINX. In accordance with the protocol model described in ISO/IEC 11582, the Supplementary Service Control entity uses, via the Coordination Function, the services of Generic Functional Transport 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 operations 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 operations 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

D.1 SDL representation at the Home PINX for initiation of SS-WTAT

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

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 Co-ordination 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.

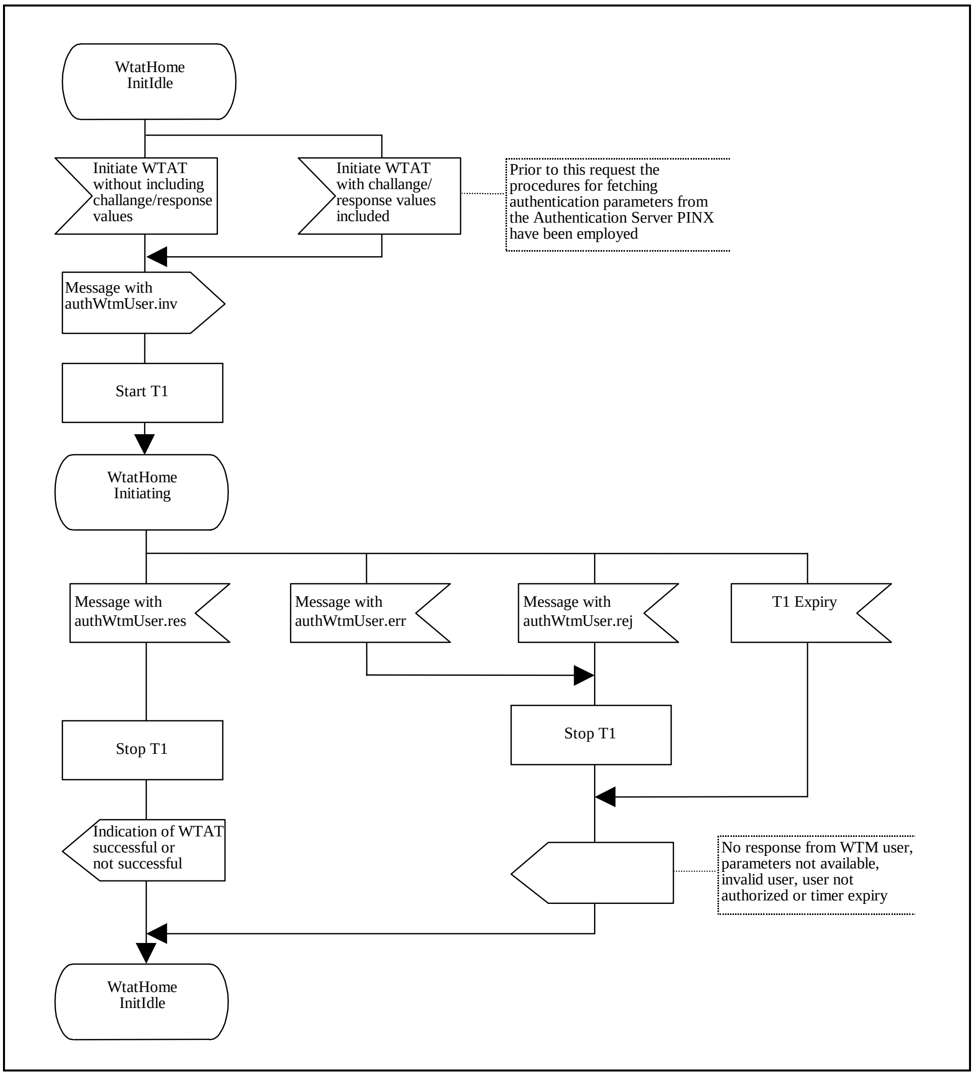
WtatHome InitIdle
Initiate WTAT without including challange/response values
Initiate WTAT with challange/ response values included
Prior to this request the procedures for fetching authentication parameters from the Authentication Server PINX have been employed
Message with authWtmUser.inv
Start T1
WtatHome Initiating
Message with authWtmUser.res
Message with authWtmUser.err
Message with authWtmUser.rej
T1 Expiry
Stop T1
Stop T1
Indication of WTAT successful or not successful
No response from WTM user, parameters not available, invalid user, user not authorized or timer expiry
WtatHome InitIdle

Figure D.1 - SDL representation at the Home PINX for initiation of SS-WTAT

D.2 SDL representation of SS-WTAT at the Home PINX for requesting authentication parameters

Figure D.2 shows the behaviour of an SS-WTAT Supplementary Service Control entity within the Home PINX for requesting authentication parameters from 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 Co-ordination 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.

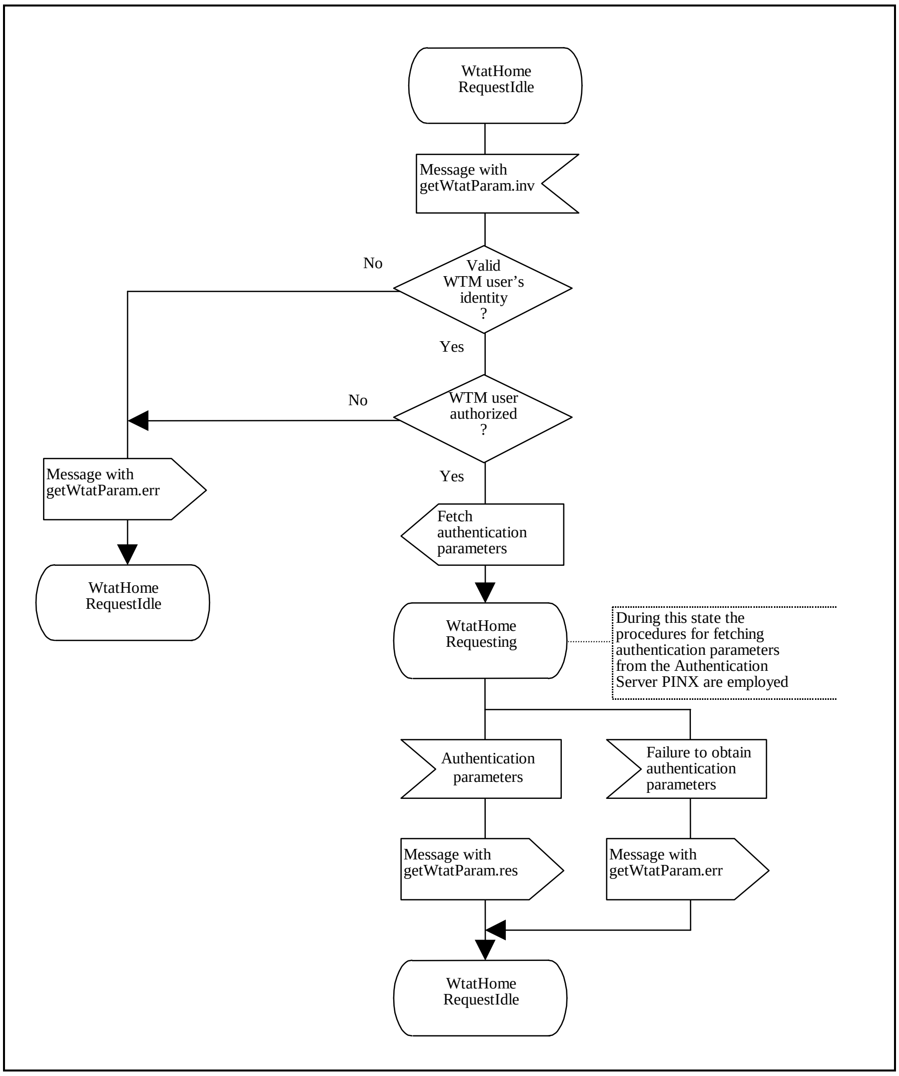
WtatHome RequestIdle
Message with getWtatParam.inv
Valid WTM user's identity ?
No
Yes
WTM user authorized ?
No
Yes
Message with getWtatParam.err
WtatHome RequestIdle
Fetch authentication parameters
WtatHome Requesting
During this state the procedures for fetching authentication parameters from the Authentication Server PINX are employed
Authentication parameters
Failure to obtain authentication parameters
Message with getWtatParam.res
Message with getWtatParam.err
WtatHome RequestIdle

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

D.3 SDL representation of SS-WTAT at the Home PINX when fetching authentication parameters

Figure D.3 shows the behaviour of an SS-WTAT 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 Co-ordination 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.

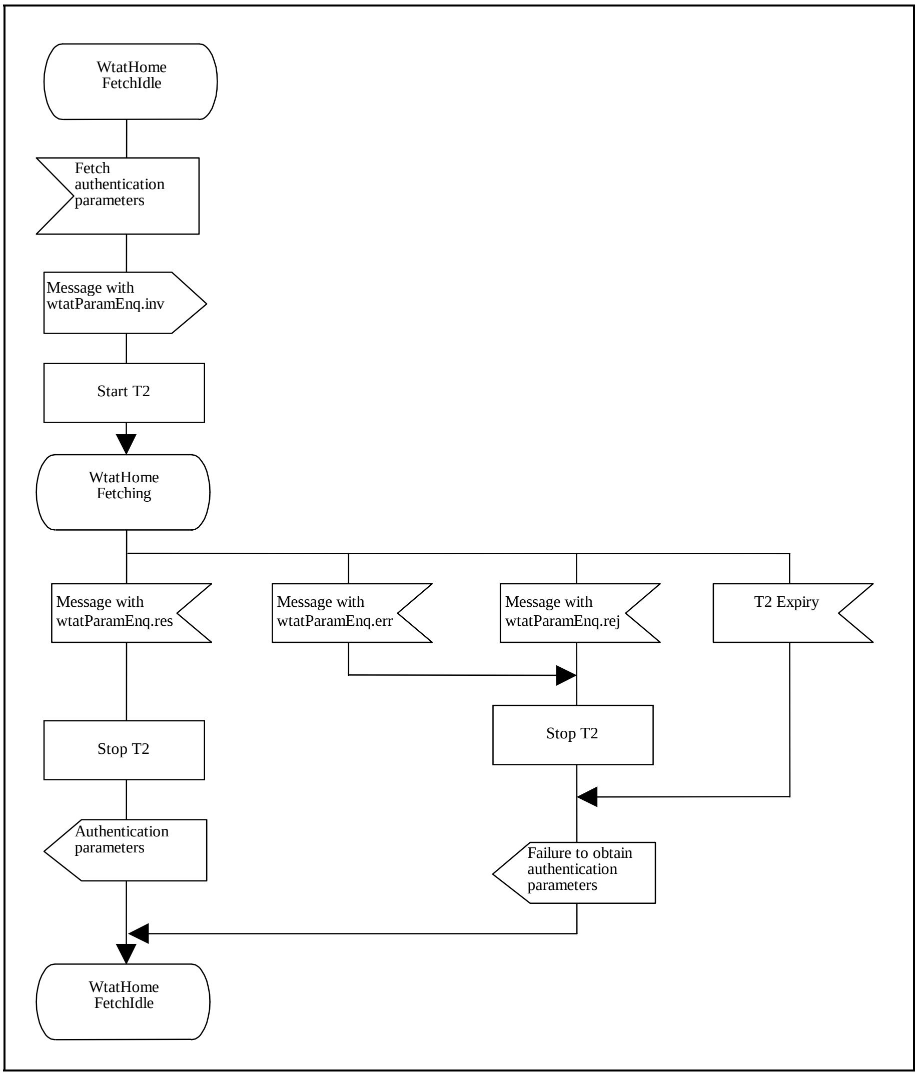
WtatHome FetchIdle
Fetch authentication parameters
Message with wtatParamEnq.inv
Start T2
WtatHome Fetching
Message with wtatParamEnq.res
Message with wtatParamEnq.err
Message with wtatParamEnq.rej
T2 Expiry
Stop T2
Stop T2
Authentication parameters
Failure to obtain authentication parameters
WtatHome FetchIdle

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

D.4 SDL representation at the Visitor PINX for execution of SS-WTAT

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

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 Co-ordination 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.

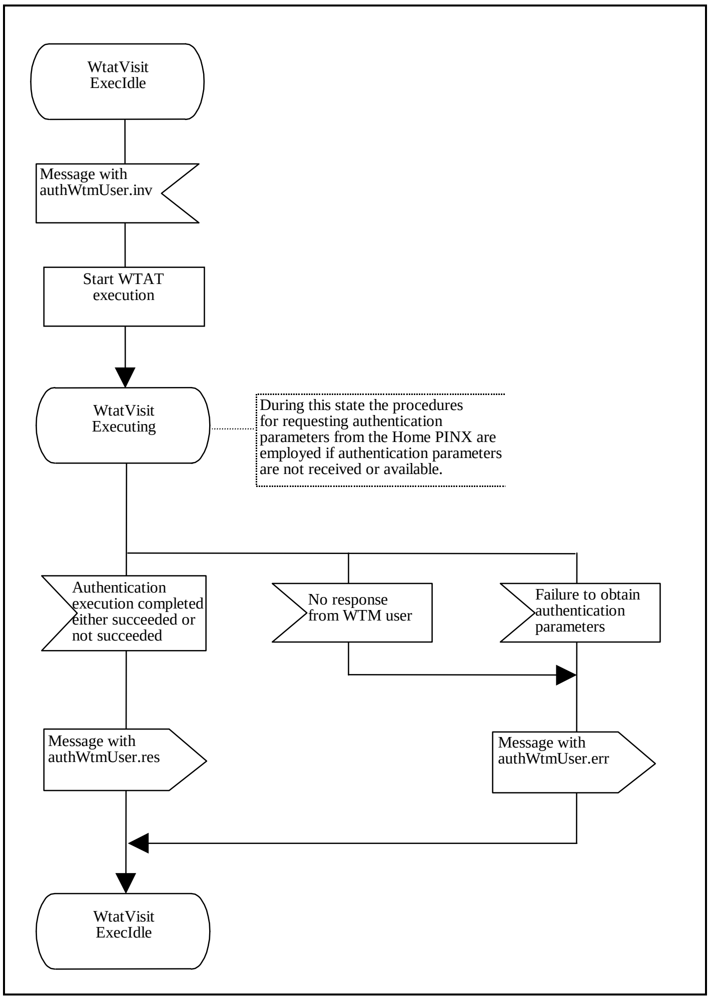
WtatVisit ExecIdle
Message with authWtmUser.inv
Start WTAT execution
WtatVisit Executing
During this state the procedures for requesting authentication parameters from the Home PINX are employed if authentication parameters are not received or available.
Authentication execution completed either succeeded or not succeeded
No response from WTM user
Failure to obtain authentication parameters
Message with authWtmUser.res
Message with authWtmUser.err
WtatVisit ExecIdle

Figure D.4 - SDL representation at the Visitor PINX for execution of SS-WTAT

D.5 SDL representation of SS-WTAT at the Visitor PINX for requesting authentication parameters

Figure D.5 shows the behaviour of an SS-WTAT 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 Co-ordination 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.

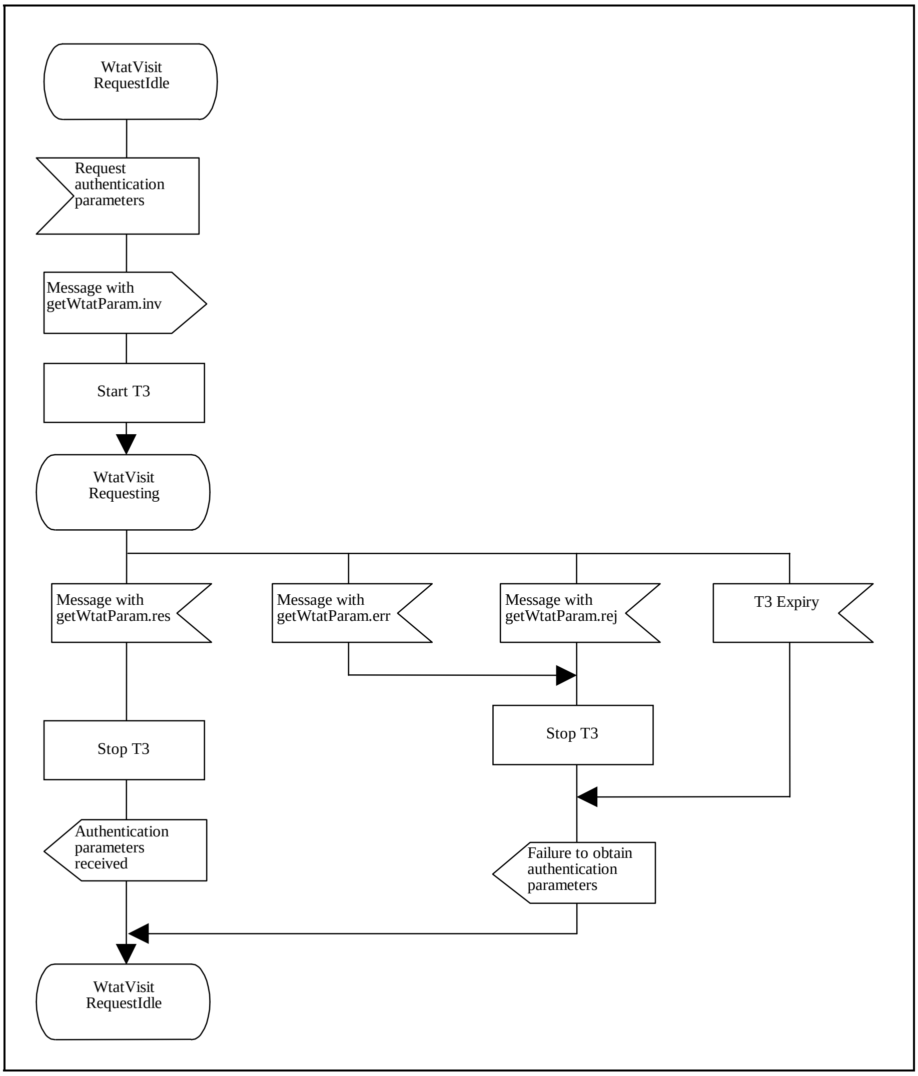
WtatVisit RequestIdle
Request authentication parameters
Message with getWtatParam.inv
Start T3
WtatVisit Requesting
Message with getWtatParam.res
Message with getWtatParam.err
Message with getWtatParam.rej
T3 Expiry
Stop T3
Stop T3
Authentication parameters received
Failure to obtain authentication parameters
WtatVisit RequestIdle

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

D.6 SDL representation of SS-WTAT at the Authentication Server PINX

Figure D.6 shows the behaviour of an SS-WTAT 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 Co-ordination 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.

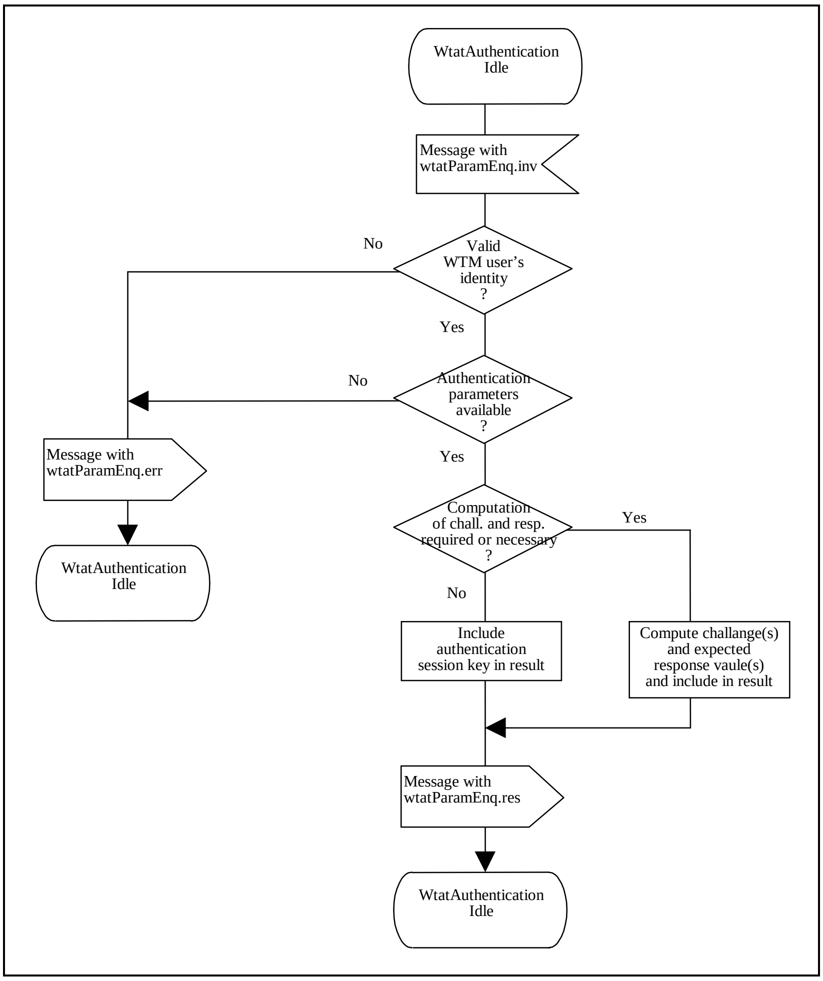
WtatAuthentication Idle
Message with wtatParamEnq.inv
Valid WTM user's identity ?
No
Yes
Authentication parameters available ?
No
Yes
Message with wtatParamEnq.err
WtatAuthentication Idle
Computation of chall. and resp. required or necessary ?
Yes
No
Include authentication session key in result
Compute challange(s) and expected response vaule(s) and include in result
Message with wtatParamEnq.res
WtatAuthentication Idle

Figure D.6 - SDL representation of SS-WTAT at the Authentication Server PINX

D.7 SDL representation of SS-WTAN at the Visitor PINX

Figure D.7 shows the behaviour of an SS-WTAN 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 WTM user.

Input signals from the right and output signals to the right represent primitives to and from the Co-ordination 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.

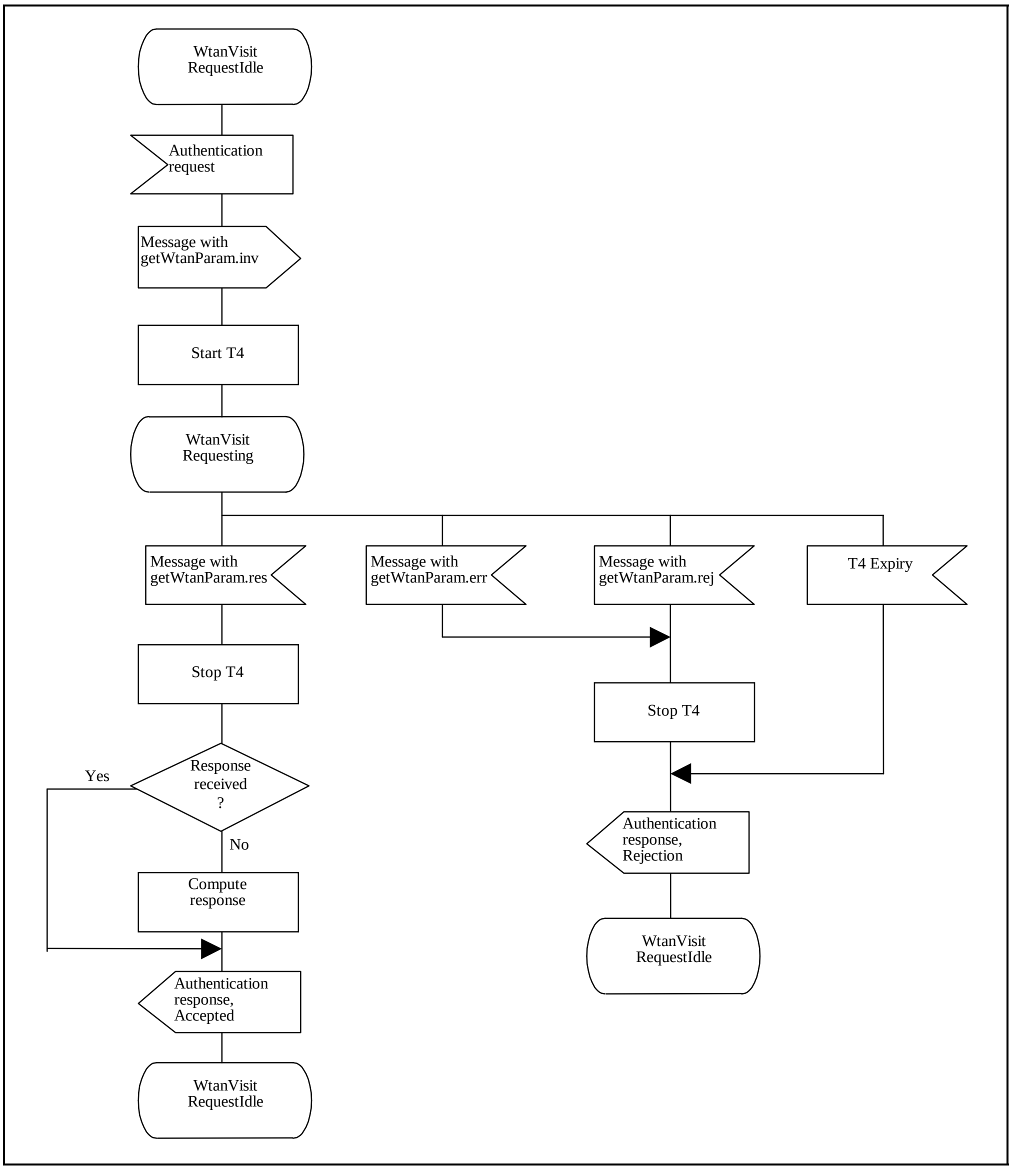
WtanVisit RequestIdle
Authentication request
Message with getWtanParam.inv
Start T4
WtanVisit Requesting
Message with getWtanParam.res
Message with getWtanParam.err
Message with getWtanParam.rej
T4 Expiry
Stop T4
Stop T4
Yes
Response received ?
No
Compute response
Authentication response, Rejection
WtanVisit RequestIdle
Authentication response, Accepted
WtanVisit RequestIdle

Figure D.7 - SDL representation of SS-WTAN at the Visitor PINX

D.8 SDL representation of SS-WTAN at the Home PINX

Figure D.8 shows the behaviour of an SS-WTAN 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 Co-ordination Function in respect of messages received and sent. Also protocol timer expiry is indicated by an input signal from the right.

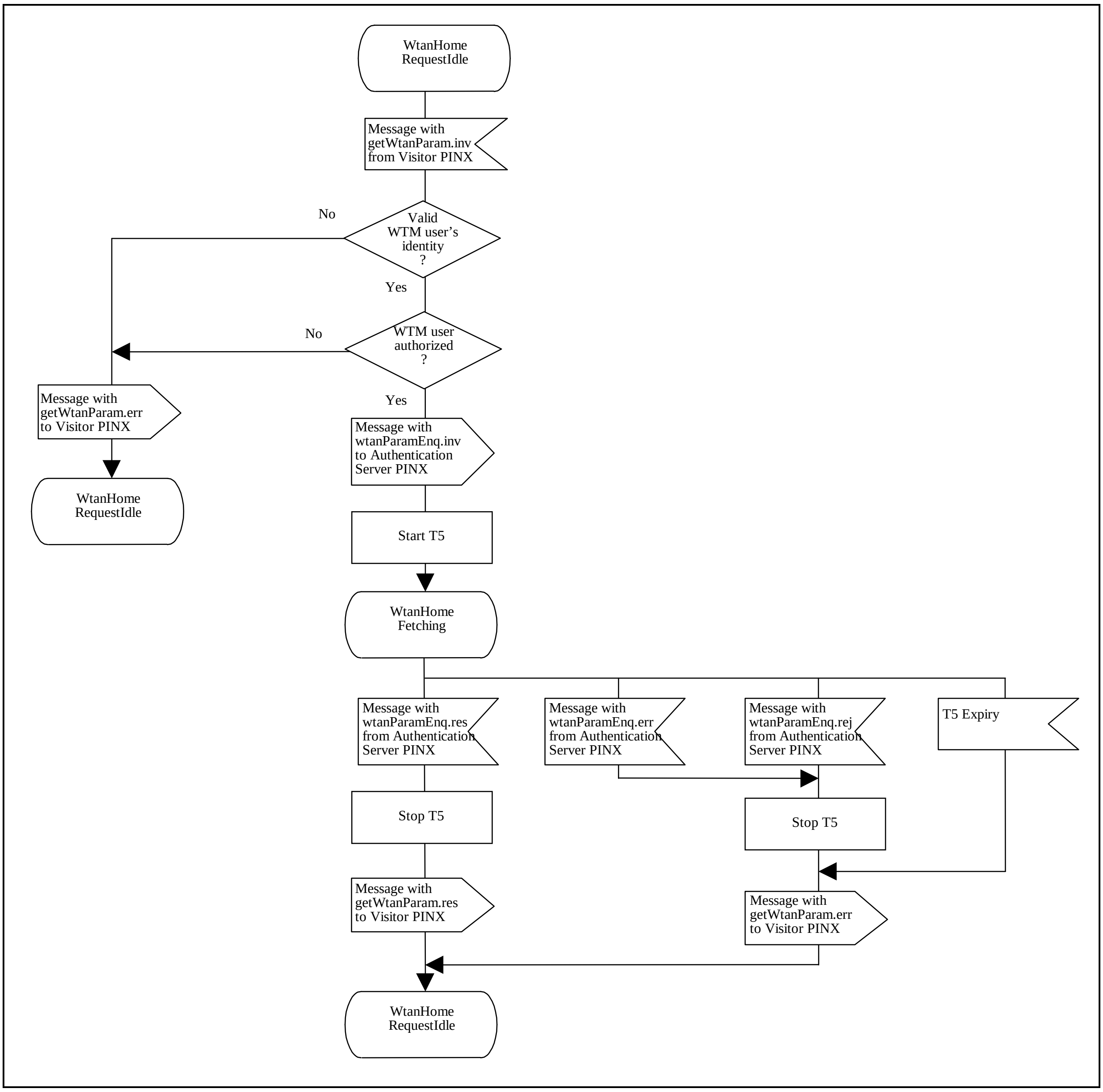
WtanHome RequestIdle
Message with getWtanParam.inv from Visitor PINX
Valid WTM user's identity ?
No
Yes
WTM user authorized ?
No
Yes
Message with getWtanParam.err to Visitor PINX
WtanHome RequestIdle
Message with wtanParamEnq.inv to Authentication Server PINX
Start T5
WtanHome Fetching
Message with wtanParamEnq.res from Authentication Server PINX
Message with wtanParamEnq.err from Authentication Server PINX
Message with wtanParamEnq.rej from Authentication Server PINX
T5 Expiry
Stop T5
Stop T5
Message with getWtanParam.res to Visitor PINX
Message with getWtanParam.err to Visitor PINX
WtanHome RequestIdle

Figure D.8 - SDL representation of SS-WTAN at the Home PINX

D.9 SDL representation of SS-WTAN at the Authentication Server PINX

Figure D.9 shows the behaviour of an SS-WTAN 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 Co-ordination 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.

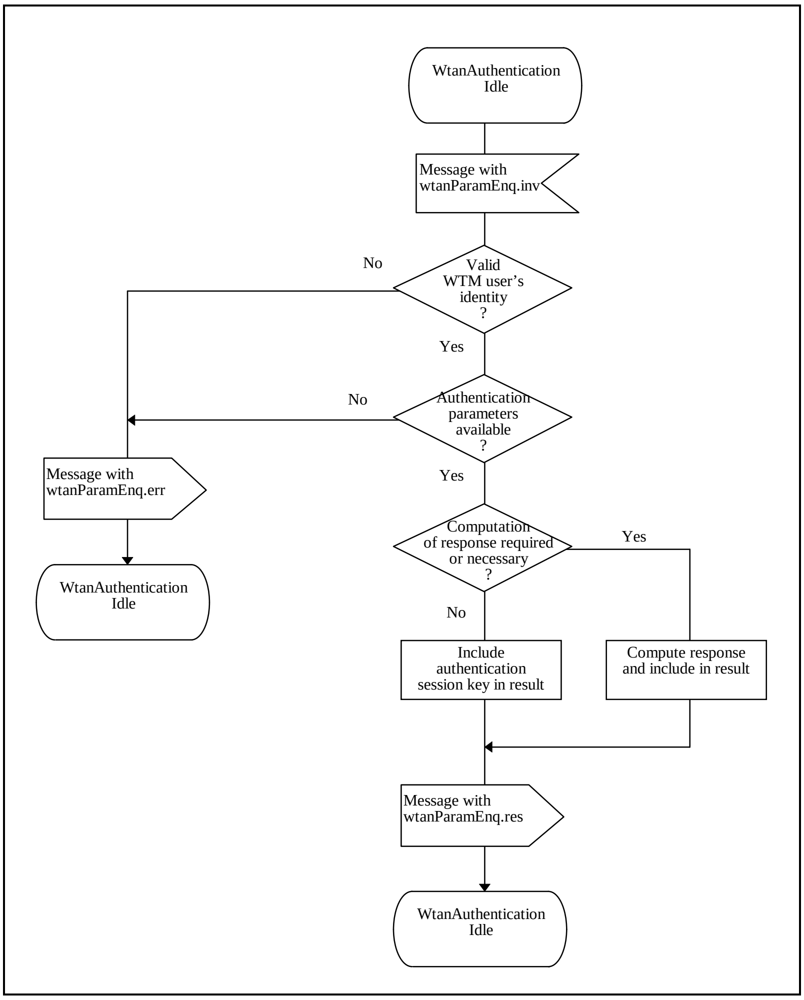
WtanAuthentication Idle
Message with wtanParamEnq.inv
Valid WTM user's identity ?
No
Yes
Authentication parameters available ?
No
Yes
Message with wtanParamEnq.err
WtanAuthentication Idle
Computation of response required or necessary ?
Yes
No
Include authentication session key in result
Compute response and include in result
Message with wtanParamEnq.res
WtanAuthentication Idle

Figure D.9 - SDL representation of SS-WTAN at the Authentication Server PINX

Annex E
(normative)

ASN.1 definitions according to ITU-T Recs. X.208 / X.209

This annex lists all ASN.1 modules as they were defined in the first edition of ISO/IEC 15433, i.e. based on ITU-T Recommendations X.208 / X.209. Starting with this edition the ASN.1 modules within ISO/IEC 15433 comply with ITU-T Recommendations X.680 / X.690. Please note that regardless of which version of these modules is used as a base of a QSIG implementation, the line encoding remains unchanged. Changes in future editions to modules based on X.680 / X.690 ASN.1 are not reflected in the modules in this annex.

Table E.1 - WTM-Authentication-Operations – based on ITU-T Recs. X.208 / X.209

```
WTM-Authentication-Operations
                        {iso standard pss1-authentication (15433) 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 standard
                              pss1-generic-procedures (11582) msi-definition (0)}
                        invalidServedUserNumber FROM General-Error-List
                              {ccitt recommendation q 950 general-error-list (1)}
                        PartyNumber FROM Addressing-Data-Elements
                              {iso(1) standard(0) pss1-generic-procedures(11582)
                              addressing-data-elements(9)};

-- The following three operations shall apply to SS-WTAT --

AuthWtmUser ::=         OPERATION         -- from Home PINX to Visitor PINX--
                        ARGUMENT          AuthWtmArg
                        RESULT            AuthWtmRes
                        ERRORS            { temporarilyUnavailable, invalidServedUserNumber,
                                            notAuthorized, paramNotAvailable, unspecified}

GetWtatParam ::=        OPERATION         -- from Visitor PINX to Home PINX --
                        ARGUMENT          WtatParamArg
                        RESULT            WtatParamRes
                        ERRORS            { invalidServedUserNumber, notAuthorized,
                                            paramNotAvailable, temporarilyUnavailable, unspecified}

WtatParamEnq ::=        OPERATION         -- from Home PINX to Authentication Server PINX--
                        ARGUMENT          WtatParamArg
                        RESULT            WtatParamRes
                        ERRORS            { invalidServedUserNumber, paramNotAvailable, unspecified}

AuthWtmArg ::=          SEQUENCE          { wtmUserId         WtmUserId,
                                          calcWtatInfo        [ 1 ] IMPLICIT CalcWtatInfo OPTIONAL,
                                          dummyExtension      DummyExtension OPTIONAL}
```

Table E.1 - WTM-Authentication-Operations – based on ITU-T Recs. X.208 / X.209 (continued)

```
AuthWtmRes ::=          SEQUENCE        { ENUMERATED    {auth-res-correct (0),
                                                         auth-res-incorrect (1) },
                                        dummyExtension   DummyExtension OPTIONAL}

WtatParamArg ::=        SEQUENCE        { wtmUserId      WtmUserId,
                                        canCompute       CanCompute OPTIONAL,
                                        authChallenge    AuthChallenge 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 --

WtatParamRes ::=        SEQUENCE        {wtatParamInfo   WtatParamInfo,
                                        dummyExtension   DummyExtension OPTIONAL}

-- The following two operations shall apply to SS-WTAN --

GetWtanParam ::=        OPERATION -- from Visitor PINX to Home PINX --
                        ARGUMENT        WtanParamArg
                        RESULT          WtanParamRes
                        ERRORS          { invalidServedUserNumber, notAuthorized,
                                          paramNotAvailable, temporarilyUnavailable, unspecified}

WtanParamEnq ::=        OPERATION -- from Home PINX to Authentication Server PINX--
                        ARGUMENT        WtanParamArg
                        RESULT          WtanParamRes
                        ERRORS          { invalidServedUserNumber, paramNotAvailable, unspecified}

WtanParamArg ::=        SEQUENCE        { wtmUserId      WtmUserId,
                                        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 --

WtmUserId ::=           CHOICE     { pisnNumber     PartyNumber,
                                        -- The PISN number of the WTM user,
                                        -- always a Complete Number.
                                     alternativeId  AlternativeId }

AlternativeId ::=       OCTET STRING(SIZE(1..20))

WtanParamRes ::=        SEQUENCE        {wtanParamInfo   WtanParamInfo,
                                        dummyExtension   DummyExtension OPTIONAL}

-- The following unconfirmed operation shall apply when interaction between SS-WTAT and ANF-WTINFO --

TransferAuthParam  ::=  OPERATION -- from Home PINX to Visitor PINX --
                        ARGUMENT        SEQUENCE {wtatParamInfo       WtatParamInfo,
                                                  dummyExtension      DummyExtension OPTIONAL}
```

Table E.1 - WTM-Authentication-Operations – based on ITU-T Recs. X.208 / X.209 (continued)

```
WtatParamInfo ::=        SEQUENCE        {authAlgorithm      AuthAlgorithm,
                                         CHOICE {
                                                authSessionKeyInfo   [ 1 ] IMPLICIT AuthSessionKeyInfo,
                                                calcWtatInfo         [ 2 ] IMPLICIT CalcWtatInfo,
                                                authKey              [ 3 ] IMPLICIT AuthKey,
                                                challLen             [ 4 ] IMPLICIT INTEGER(1..8) } }

AuthKey ::=              OCTET STRING (SIZE(1..16))  -- Authentication key --

WtanParamInfo ::=        CHOICE     {authSessionKeyInfo      [ 1 ] IMPLICIT AuthSessionKeyInfo,
                                    calcWtanInfo             [ 2 ] IMPLICIT CalcWtanInfo}

AuthSessionKeyInfo ::=   SEQUENCE        {authSessionKey     AuthSessionKey,
                                         calculationParam    CalculationParam}

CalcWtatInfo ::=         SEQUENCE SIZE(1..5) OF CalcWtatInfoUnit

CalcWtatInfoUnit ::=     SEQUENCE        {authChallenge      AuthChallenge,
                                         authResponse        AuthResponse,
                                         derivedCipherKey    [1] IMPLICIT DerivedCipherKey OPTIONAL,
                                         calculationParam    [2] IMPLICIT CalculationParam OPTIONAL}
                                         -- included if required by the authentication algorithm in use --

CalcWtanInfo ::=         SEQUENCE        {authResponse       AuthResponse,
                                         calculationParam    CalculationParam OPTIONAL}
                                         -- included if required by the authentication algorithm in use --

DummyExtension ::=       CHOICE     {extension           [5] IMPLICIT Extension,
                                    sequOfExtn           [6] IMPLICIT SEQUENCE OF Extension}

AuthAlgorithm ::=        SEQUENCE        { authAlg       INTEGER { ct2 (0), dect (1), gsm (2), pci (3),
                                                                  pwt (4), us-gsm (5), phs (6),
                                                                  tetra (7) } (0..255),
                                         ANY DEFINED BY authAlg OPTIONAL}

AuthChallenge ::=        OCTET STRING (SIZE(1..8))   -- Randomly generated parameter --

AuthResponse ::=         OCTET STRING (SIZE(1..4))   -- WTAT: Expected response value --
                                                     -- WTAN: 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 WTM user during --
                                                     -- both WTAT and WTAN. --

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--
```

Table E.1 - WTM-Authentication-Operations – based on ITU-T Recs. X.208 / X.209 (concluded)

```
authWtmUser             AuthWtmUser           ::=     localValue 72
getWtatParam            GetWtatParam          ::=     localValue 73
wtatParamEnq            WtatParamEnq          ::=     localValue 74
getWtanParam            GetWtanParam          ::=     localValue 75
wtanParamEnq            WtanParamEnq          ::=     localValue 76
transferAuthParam       TransferAuthParam     ::=     localValue 77

notAuthorized           ERROR                 ::=     localValue 1007
paramNotAvailable       ERROR                 ::=     localValue 1017
temporarilyUnavailable  ERROR                 ::=     localValue 1000
unspecified             Unspecified           ::=     localValue 1008

Unspecified ::=         ERROR       PARAMETER Extension

END                     -- of WTM-Authentication-Operations
```

ICS 33.040.35

Price based on 48 pages