INTERNATIONAL STANDARD

ISO/IEC 15432

First edition
1999-09-15

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)

Technologies de l'information — Télécommunications et échange d'information entre systèmes — Réseau privé à intégration de services — Spécification, modèle fonctionnel et flux d'information — Services supplémentaires d'authentification de terminal sans fil (WTAT et WTAN)

Reference number
ISO/IEC 15432:1999(E)

Contents

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. 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.

International Standard ISO/IEC 15432 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*.

Annex A of this International Standard is for information only.

Introduction

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

This particular International Standard specifies the WTAT and WTAN supplementary services.

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)

1 Scope

This International Standard specifies the Authentication supplementary services, which are applicable to various basic services supported by Private Integrated Services Networks (PISN). Basic services are specified in ISO/IEC 11574.

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 supplementary services are based on the challenge and response method of authentication. Authentication algorithms to be used by these two supplementary services (SS-WTAT and SS-WTAN) are outside the scope of this International Standard. This International Standard provides the information flows to convey the security parameters.

Supplementary service specifications are produced in three stages, according to the method described in CCITT Recommendation I.130. This International Standard contains the stage 1 and stage 2 specifications of SS-WTAT and SS-WTAN. The stage 1 specification (clause 6 and 7) specifies the supplementary service as seen by users of PISNs. The stage 2 specification (clause 8 and 9) identifies the functional entities involved in the supplementary service and the information flows between them.

2 Conformance

In order to conform to this International Standard, a stage 3 International Standard shall specify signalling protocols and equipment behaviour that are capable of being used in a PISN which supports the supplementary service specified in this International Standard. This means that, to claim conformance, a stage 3 International Standard is required to be adequate for the support of those aspects of clause 6 and 7 (stage 1) and clause 8 and 9 (stage 2) which are relevant to the interface or equipment to which the stage 3 International Standard applies.

3 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this International Standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/IEC 11571:1994, *Information technology - Telecommunications and information exchange between systems - Numbering and sub-addressing in private integrated services networks.*

ISO/IEC 11574:1994, *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).*

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

CCITT 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. Z.100:1993, *Specification and Description Language.*

4 Definitions

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

4.1 External definitions

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

- Additional Network Feature (ANF) (ISO/IEC project 1.06.57.09.02, 'WTLR')
- Authentication (ISO/IEC project 1.06.57.09.02, 'WTLR')
- Basic service (ITU-T Rec. I.210)
- Wireless Terminal Mobility (WTM) (ISO/IEC project 1.06.57.09.02, 'WTLR')
- Fixed Part (FP) (ISO/IEC project 1.06.57.09.02, 'WTLR')
- Home-PINX (ISO/IEC project 1.06.57.09.02, 'WTLR')
- PISN authority (ISO/IEC project 1.06.57.09.02, 'WTLR')
- PISN user (ISO/IEC project 1.06.57.09.02, 'WTLR')
- Private Integrated Services Network (PISN) (ISO/IEC 11579-1)
- Private Integrated Services Network Exchange (PINX) (ISO/IEC 11579-1)
- Service (ITU-T Rec. I.112)
- Signalling (ITU-T Rec. I.112)
- Supplementary Service (ITU-T Rec. I.210)
- User (ISO/IEC 11574)
- WTM user's identity (ISO/IEC 15428, 'WTLR')
- Visitor PINX (ISO/IEC project 1.06.57.09.02,'WTLR')

4.2 Other definitions

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

Wireless Terminal: A physical entity that provides access to the telecommunication services of a PISN via a radio interface.

WTAN user: A user of the supplementary service SS-WTAN.

WTAT user: A user of the supplementary service SS-WTAT.

5 List of acronyms

ANF	Additional Network Feature
CC	Call Control (functional entity)
CCA	Call Control Agent (functional entity)
FE	Functional Entity
FP	Fixed Part
ISDN	Integrated Services Digital Network

PINX Private Integrated Services Network Exchange

PISN Private Integrated Services Network

SDL Specification and Description Language

SS Supplementary Service

SS-WTAT Supplementary Service - Authentication of a WTM user

SS-WTAN Supplementary Service - Authentication of a PISN

WT Wireless Terminal

WTM Wireless Terminal Mobility

6 SS-WTAT stage 1 specification

6.1 Description

6.1.1 General description

Authentication of a Wireless Terminal (SS-WTAT) 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. The received response is compared with the expected response.

6.1.2 Qualifications on applicability to telecommunication services

SS-WTAT is applicable to all basic services defined in ISO/IEC 11574.

6.2 Procedure

6.2.1 Provision/withdrawal

SS-WTAT shall be provided and withdrawn by arrangement with the PISN authority.

6.2.2 Normal procedures

6.2.2.1 Activation/deactivation/registration/interrogation

SS-WTAT shall be activated on provision and deactivated on withdrawal.

Registration and interrogation are not applicable to this supplementary service.

6.2.2.2 Invocation and operation

SS-WTAT may be invoked at any time, e.g. when the WTM user requests a basic or supplementary service.

The operation of SS-WTAT is based on the 'challenge and response' method of authentication. Upon invocation of this service, the PISN sends specific information (challenge) to the WTM user and awaits a response. If the response from the WTM user is the expected one, then authentication has passed successfully. If the response is not the expected response, the PISN may take any action as appropriate.

6.2.3 Exceptional procedures

6.2.3.1 Activation/deactivation/registration/interrogation

Not applicable

6.2.3.2 Invocation and operation

If SS-WTAT cannot be performed, the PISN may reject or limit the service to the WTM user.

Possible reasons are:

- Incorrect authentication parameters;
- WT not accessible.

6.3 Interaction with other supplementary services and ANFs

Interactions with other supplementary services and ANFs for which PISN International Standards were available at the time of publication of this International Standard are specified below.

6.3.1 Calling Line Identification Presentation (SS-CLIP)

No interaction

6.3.2 Connected Line Identification Presentation (SS-COLP)

No interaction

6.3.3 Calling/Connected Line Identification Restriction (SS-CLIR)

No interaction

6.3.4 Calling Name Identification Presentation (SS-CNIP)

No interaction

6.3.5 Connected Name Identification Presentation (SS-CONP)

No interaction

6.3.6 Calling/Connected Name Identification Restriction (SS-CNIR)

No interaction

6.3.7 Completion of Calls to Busy Subscriber (SS-CCBS)

No interaction

6.3.8 Completion of Calls on No Reply (SS-CCNR)

No interaction

6.3.9 Call Transfer (SS-CT)

No interaction

6.3.10 Call Forwarding Unconditional (SS-CFU)

No interaction

6.3.11 Call Forwarding Busy (SS-CFB)

No interaction

6.3.12 Call Forwarding No Reply (SS-CFNR)

No interaction

6.3.13 Call Deflection (SS-CD)

No interaction

6.3.14 Path Replacement (ANF-PR)

No interaction

6.3.15 Call offer (SS-CO)

No interaction

6.3.16 Call intrusion, (SS-CI)

No interaction

6.3.17 Do Not Disturb (SS-DND)

No interaction

6.3.18 Do Not Disturb Override (SS-DNDO)

No interaction

6.3.19 Advice of Charge (SS-AOC)

No interaction

6.3.20 Recall (SS-RE)

No interaction

6.3.21 Interaction with Call Interception (ANF-CINT)

No interaction

6.3.22 Interaction with Transit Counter (ANF-TC)

No interaction

6.3.23 Interaction with Route Restriction Class (ANF-RRC)

No interaction

6.3.24 Message waiting indication (SS-MWI)

No interaction

6.3.25 Wireless terminal location registration (SS-WTLR)

SS-WTLR may cause the invocation of SS-WTAT.

6.3.26 Wireless terminal information exchange (ANF-WTINFO)

No interaction

6.3.27 Wireless terminal incoming call (ANF-WTMI)

ANF-WTMI may cause the invocation of SS-WTAT.

6.3.28 Wireless terminal outgoing call (ANF-WTMO)

ANF-WTMO may cause the invocation of SS-WTAT.

6.3.29 Authentication of network (SS-WTAN)

No interaction

6.4 Interworking considerations

Not applicable

6.5 Overall SDL

Figure 1 contains the dynamic description of SS-WTAT using the Specification and Description Language (SDL) defined in ITU-T Rec. Z.100. The SDL process represents the behaviour of the PISN in providing SS-WTAT. Input signals from the left and output signals to the left represent internal stimuli within the PISN. Input signals from the right represent primitives from the WTM user. Output signals to the right represent primitives to the WTM user.

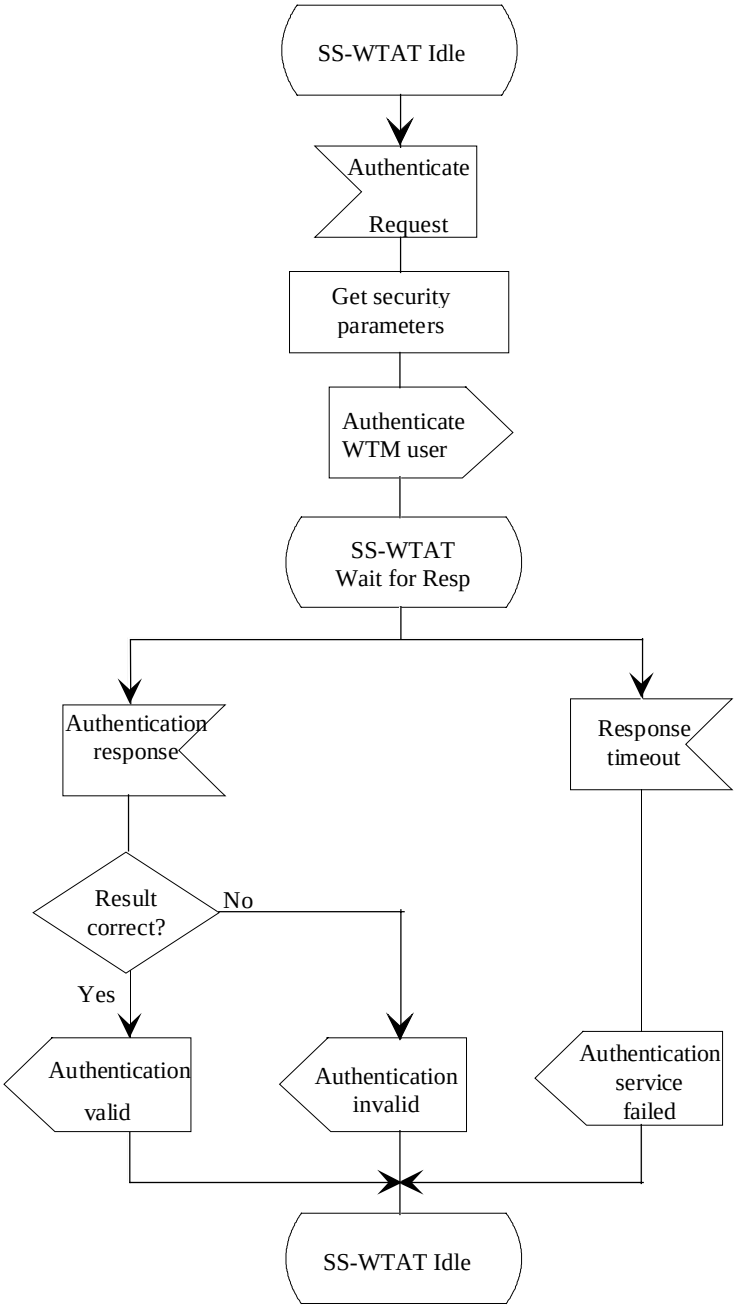

Figure 1: SS-WTAT, overall SDL

7 SS-WTAN stage 1 specification

7.1 Description

7.1.1 General description

SS-WTAN 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. The received response is compared with the expected response.

7.1.2 Qualifications on applicability to telecommunication services

SS-WTAN is applicable to all basic services defined in ISO/IEC 11574.

7.2 Procedure

7.2.1 Provision/withdrawal

SS-WTAN shall be provided and withdrawn by arrangement with the PISN authority.

7.2.2 Normal procedures

7.2.2.1 Activation/deactivation/registration/interrogation

SS-WTAN shall be activated on provision and deactivated on withdrawal.

Registration and interrogation are not applicable to this supplementary service.

7.2.2.2 Invocation and operation

SS-WTAN may be invoked by the WTM user at any time, e.g. before accepting certain instructions from the PISN.

The operation of SS-WTAN is based on the 'challenge and response' method of authentication. Upon invocation of this service, the WTM user sends specific information (challenge) to the PISN and awaits a response. If the response from the PISN is the expected one, then authentication has passed successfully. If the response is not the expected response, the WTM user may take any action as appropriate.

7.2.3 Exceptional procedures

7.2.3.1 Activation/deactivation/registration/interrogation

Not applicable

7.2.3.2 Invocation and operation

If SS-WTAN cannot be performed, the WTM user may reject instructions from the PISN.

Possible reasons are:

- Incorrect authentication parameters;
- SS-WTAN not available.

7.3 Interaction with other supplementary services and ANFs

Interactions with other supplementary services and ANFs for which PISN International Standards were available at the time of publication of this International Standard are specified below.

7.3.1 Calling Line Identification Presentation (SS-CLIP)

No interaction

7.3.2 Connected Line Identification Presentation (SS-COLP)

No interaction

7.3.3 Calling/Connected Line Identification Restriction (SS-CLIR)

No interaction

7.3.4 Calling Name Identification Presentation (SS-CNIP)

No interaction

7.3.5 Connected Name Identification Presentation (SS-CONP)

No interaction

7.3.6 Calling/Connected Name Identification Restriction (SS-CNIR)

No interaction

7.3.7 Completion of Calls to Busy Subscriber (SS-CCBS)

No interaction

7.3.8 Completion of Calls on No Reply (SS-CCNR)

No interaction

7.3.9 Call Transfer (SS-CT)

No interaction

7.3.10 Call Forwarding Unconditional (SS-CFU)

No interaction

7.3.11 Call Forwarding Busy (SS-CFB)

No interaction

7.3.12 Call Forwarding No Reply (SS-CFNR)

No interaction

7.3.13 Call Deflection (SS-CD)

No interaction

7.3.14 Path Replacement (ANF-PR)

No interaction

7.3.15 Call offer (SS-CO)

No interaction

7.3.16 Call intrusion, (SS-CI)

No interaction

7.3.17 Do Not Disturb (SS-DND)

No interaction

7.3.18 Do Not Disturb Override (SS-DNDO)

No interaction

7.3.19 Advice of Charge (SS-AOC)

No interaction

7.3.20 Recall (SS-RE)

No interaction

7.3.21 Interaction with Call Interception (ANF-CINT)

No interaction

7.3.22 Interaction with Transit Counter (ANF-TC)

No interaction

7.3.23 Interaction with Route Restriction Class (ANF-RRC)

No interaction

7.3.24 Message waiting indication (SS-MWI)

No interaction

7.3.25 Wireless **terminal location registration (SS-WTLR)**

No interaction

7.3.26 Wireless **terminal information exchange (ANF-WTINFO)**

No interaction

7.3.27 Wireless **terminal incoming call (ANF-WTMI)**

No interaction

7.3.28 Wireless **terminal outgoing call (ANF-WTMO)**

No interaction

7.3.29 Authentication of wireless terminal (SS-WTAT)

No interaction

7.4 Interworking considerations

Not applicable

7.5 Overall SDL

Figure 2 contains the dynamic description of SS-WTAN using the Specification and Description Language (SDL) defined in ITU-T Rec. Z.100. The SDL process represents the behaviour of the PISN in providing SS-WTAN.

Input signals from the right represent primitives from the WTM user's current access. Output signals to the right represent primitives to the WTM user's current access.

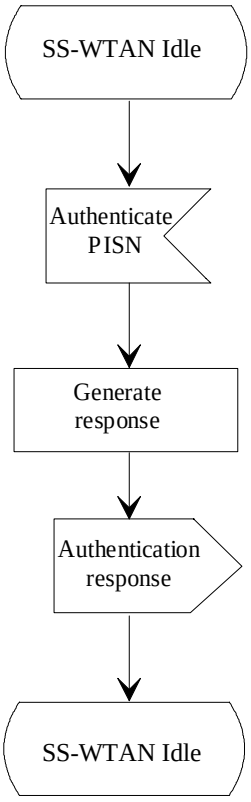

Figure 2: SS-WTAN, overall SDL

8 SS-WTAT stage 2 specification

8.1 Functional model

8.1.1 Functional model description

The functional model shall comprise the following functional entities:

FE1: WTAT initiator
FE2: Authentication detection and control
FE3: Authentication execution
FE4: WTM served user agent
FE5 Home location control
FE6 Authentication centre

The following functional relationships shall exist between these functional entities:

ra between FE1 and FE2
rb between FE2 and FE3
rc between FE3 and FE4
rd between FE2 and FE5
re between FE5 and FE6

Figure 3 shows these FEs and relationships.

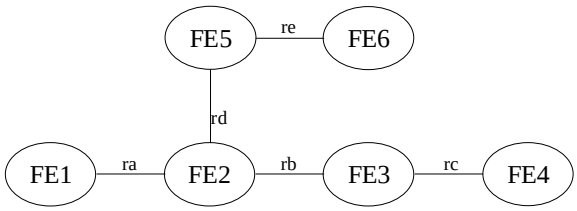

Figure 3: Functional model for SS-WTAT

8.1.2 Description of functional entities

8.1.2.1 WTAT initiator, FE1

This FE initiates a request for authentication of the WTM user and forwards this to FE2.

8.1.2.2 Authentication detection and control, FE2

This FE detects a request for authentication from FE1 and requests the necessary parameters, if needed, from FE5. FE2 may generate a challenge and an expected response. It then requests FE3 to execute the authentication of the specified WTM user.

8.1.2.3 Authentication execution, FE3

This FE receives the request to authenticate a WTM user. It computes a challenge and an expected response, if these have not been provided. It receives responses to the challenges from FE4.

8.1.2.4 WTM served user agent, FE4

This entity forwards the challenge to a WTM user and forwards any received responses from the WTM user to FE3.

8.1.2.5 Home location, FE5

This FE requests authentication parameters from FE6, on request from FE2.

8.1.2.6 Authentication centre, FE6

This FE provides FE5 with authentication parameters related to a WTM user on request from FE2. It may compute a challenge and an expected response based on the authentication parameters, on request.

8.1.3 Relationship of functional model to basic call functional model

All information flows are independent of basic call flows.

8.2 Information flows

8.2.1 Definition of information flows

In the tables listing the service elements in information flows, the column headed "Request" indicates which of these service elements are mandatory (M) and which are optional (O) in a request/indication information flow, and the column headed "Confirm" indicates which of these service elements are mandatory (M) and which are optional (O) in a response/confirmation information flow.

8.2.1.1 AP-ENQ

AP-ENQ is a confirmed information flow across re from FE5 to FE6 which requests FE6 to provide authentication parameters of a WTM user.

Table 1 lists the service elements within the AP-ENQ information flow.

Table 1: Content of AP-ENQ

Service Elements	Allowed Values	Request	Confirm
WTM user's identity	note 1	M	
Authentication Service	SS-WTAT	M	
Challenge		O	
Computation possible	Yes/No	O	
Result	Accepted/Rejected		M
Authentication Parameters			O (note 2)
Cause of rejection	Parameters not available		O (note 3)

NOTE 1: This service element may be the WTM users complete PISN number or an equivalent unique identifier.

NOTE 2: The authentication parameters shall be provided if the request is accepted.

NOTE 3: This service element may be included only if the service is rejected.

NOTE The Authentication parameters in AP-ENQ-confirm contain either a set of parameters sufficient to compute a challenge and/or response by another FE or both a challenge and expected response.

8.2.1.2 AU-WTM

AU-WTM is a confirmed information flow across ra from FE1 to FE2 which conveys a request to authenticate a WTM user.

Table 2 lists the service elements within the AU-WTM information flow.

Table 2: Content of AU-WTM

Service Elements	Allowed Values	Request	Confirm
WTM user's identity		M	
Result	Accept/Reject		M
Accept Result	WT auth result correct		O (note 1)
	WT auth result incorrect		
Cause of rejection	WT not accessible		O (note 2)

NOTE 1: This service element shall only be included if the service is accepted.

NOTE 2: This service element may be included only if the service is rejected.

8.2.1.3 AU-PARM

AU-PARM is a confirmed information flow across rd from FE2 to FE5 which requests FE5 to provide authentication parameters of a WTM user.

Table 3 lists the service elements within the AU-PARM information flow.

Table 3: Content of AU-PARM

Service Elements	Allowed Values	Request	Confirm
WTM user's identity		M	
Authentication Service	SS-WTAT	M	
Challenge		O	
Computation possible	Yes/No	O	
Result	Accepted/Rejected		M
Authentication Parameters			O (note 1)
Cause of rejection	WTM user unknown WTM user not authorised for SS-WTAT Parameters not available		O (note 2)
NOTE 1: The authentication parameters shall be provided if the request is accepted			
NOTE 2: This service element may be included only if the service is rejected.			

NOTE The Authentication parameters in AU-PARM-confirm contain either a set of parameters sufficient to compute a challenge and/or response by another FE or both a challenge and expected response.

8.2.1.4 AUTH

AUTH is a confirmed information flow across rb from FE2 to FE3 which requests FE3 to authenticate the WTM user. The response indicates the authentication result.

Table 4 lists the service elements within the AUTH information flow.

Table 4: Content of AUTH

Service Elements	Allowed Values	Request	Confirm
WTM user's identity		M	
Authentication Parameters		M	
Result	Accept/Reject		M
Accept result	WT auth result correct WT auth result incorrect		O (note 1)
Cause of rejection	WT not accessible		O (note 2)
NOTE 1: This service element shall only be included if the service is accepted.			
NOTE 2: This service element may be included only if the service is rejected.			

NOTE The Authentication parameters in AUTH-request contain both a challenge and expected response.

8.2.1.5 CHALL-WT

CHALL-WT is a confirmed information flow across rc from FE3 to FE4 which indicates to FE4 that it shall forward the challenge to the WTM user.

Table 5 lists the service elements within the CHALL-WT information flow.

Table 5: Content of CHALL-WT

Service Elements	Allowed Values	Request	Confirm
WTM user's identity		M	
Challenge		M	
Result	Accept/Reject		M
Response value			O (note 1)
Cause of rejection	WT not accessible		O (note 2)
NOTE 1: The Response value service element shall be included if the service is accepted.			
NOTE 2: This service element may be included only if the service is rejected.			

8.2.2 Relationship of information flows to basic call information flows

All information flows are independent of basic call flows.

8.2.3 Examples of information flow sequences

A stage 3 International Standard for WTAT shall provide signalling procedures in support of the information flow sequences specified below. In addition, signalling procedures should be provided to cover other sequences arising from error situations, interactions with basic call, interactions with other supplementary services, different topologies, etc.

In the figures, SS-WTAT information flows are represented by solid arrows and basic call information flows are represented by broken arrows. An ellipse embracing two information flows indicates that the two information flows occur simultaneously. Within a column representing an SS-WTAT functional entity, the numbers refer to functional entity actions listed in 8.3. The following abbreviations are used:

req request

ind indication

resp response

conf confirmation

8.2.3.1 Successful authentication of a WTM user (parameters available locally)

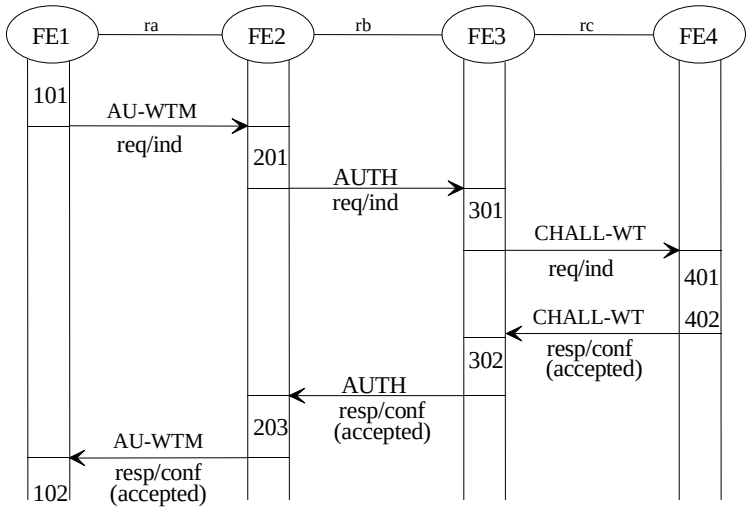

Figure 4 shows the information flow for successful authentication of a WTM user with parameters being available locally in FE2.

Figure 4: Successful case with parameters available locally in FE2

8.2.3.2 Successful authentication of a WTM user (parameters retrieved from FE5)

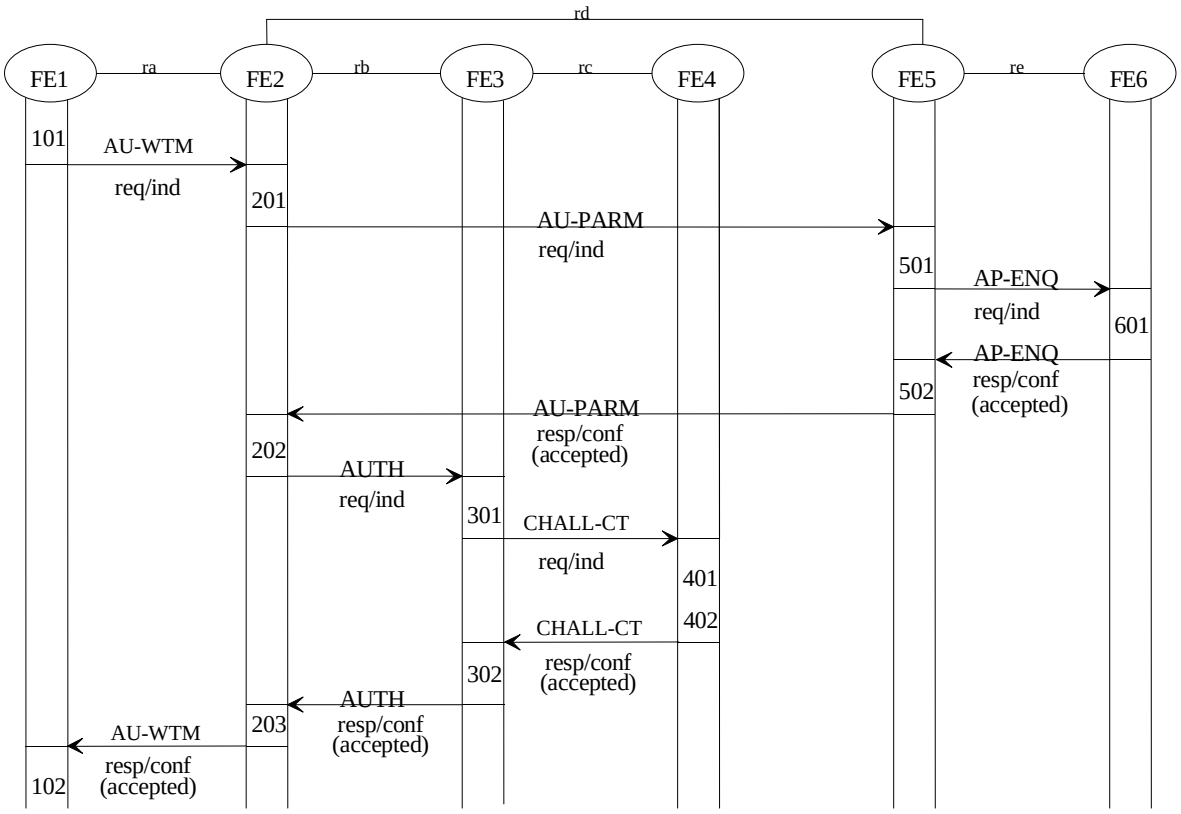

Figure 5 shows the information flow for successful authentication of a WTM user. The authentication parameters are retrieved from FE5 by FE2 prior to continuing with the authentication.

Figure 5: Successful case with parameters retrieved from FE5 by FE2

8.2.3.3 Unsuccessful authentication of a WTM user (rejection from FE4)

Figure 6 shows the information flow for unsuccessful authentication of a WTM user where a rejection is received from FE4 (e.g. WT not accessible or an internal service time out).

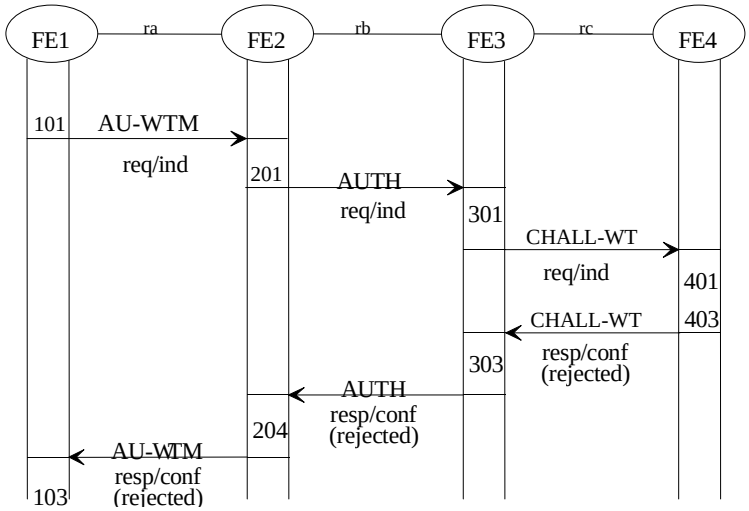

Figure 6: Unsuccessful case, rejection from FE4

NOTE: The parameters for SS-WTAT may be available either locally at FE2 (as shown in figure 4) or retrieved from FE5 (as shown in figure 5).

8.2.3.4 Unsuccessful authentication of a WTM user (parameter retrieval rejection from FE5)

Figure 7 the information flow for unsuccessful authentication of a WTM user where a rejection is received from FE5 (e.g. incorrect WTM user's identity).

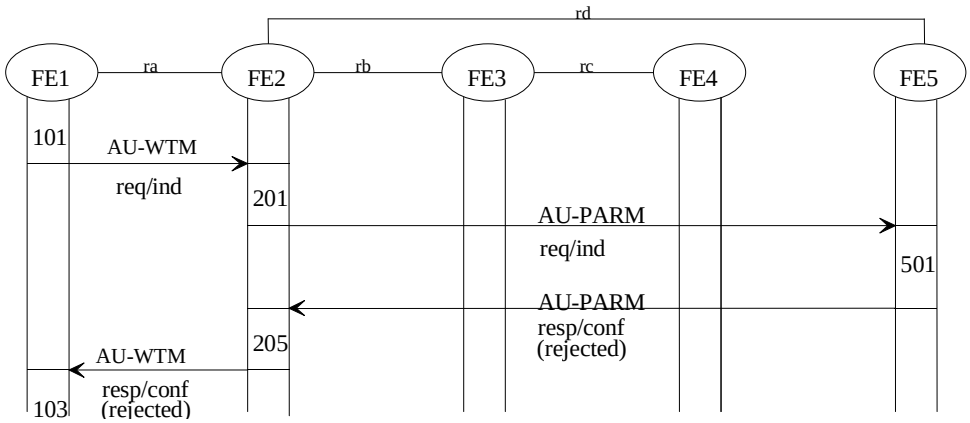

Figure 7: Unsuccessful case, rejection from FE5

8.2.3.5 Unsuccessful authentication of a WTM user (parameter retrieval rejection from FE6)

Figure 8 shows the information flow for unsuccessful authentication of a WTM user where a rejection is received from FE6 (e.g. parameters not available).

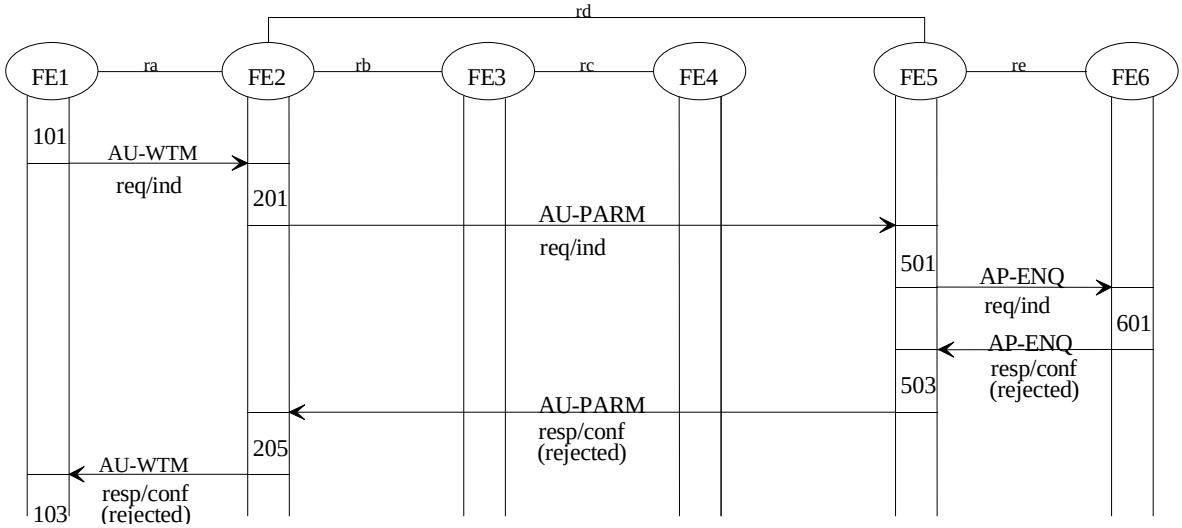

Figure 8: Unsuccessful case, rejection from FE6

8.3 Functional entity actions

The following FE actions shall occur at the points indicated in the figures of 8.2.3.

8.3.1 Functional entity actions of FE1

101 Receive a request to authenticate a WTM user, and send AU-WTM-request to FE2.

102 Receive AU-WTM-confirm (accepted) from FE2 and indicate Auth. WTM user confirmed to the initiating entity.

103 Receive AU-WTM-confirm (rejected) from FE2 and indicate Auth. WTM user failed to the initiating entity.

8.3.2 Functional entity actions of FE2

201 Receive AU-WTM-indication from FE1 and test if parameters are locally available.
If the parameters are available then send AUTH-request to FE3.
If the parameters are not available then send AU-PARM-request to FE5.

202 Receive AU-PARM confirm (accepted) from FE5 and send AUTH-request to FE3

203 Receive AUTH-confirm (accepted) from FE3 and send AU-WTM-response (accepted) to FE1.

204 Receive AUTH-confirm (rejected) from FE3 and send AU-WTM-response (rejected) to FE1.

205 Receive AU-PARM-confirm (rejected) from FE5 and send AU-WTM-response (rejected) to FE1.

8.3.3 Functional entity actions of FE3

301 Receive AUTH-indication from FE2. Test if computation of a challenge and expected response is required.
If required then compute a challenge and send CHALL-WT-request to FE4.
If not required then forward the challenge computed by FE6 to FE4 in CHALL-WT-request.

302 Receive CHALL-WT-confirm (accepted) from FE4 and test if the result is correct.
If the result is correct then send AUTH-response (accepted) to FE2. with "WT auth result correct".
If the result is incorrect then send AUTH-response (accepted) to FE2 with "WT auth. result incorrect".

303 Receive CHALL-WT-confirm (rejected) from FE4 and send AUTH-response (rejected) to FE2.

8.3.4 Functional entity actions of FE4

401 Receive CHALL-WT-indication from FE3 and send the challenge to the WTM user. Start the service timer.

402 Receive a response from the WTM user and send CHALL-WT-response (accepted) to FE3. Stop the service timer.

403 On internal time out send CHALL-WT-confirm (rejected) to FE3.

8.3.5 Functional entity actions of FE5

501 Receive AU-PARM-indication from FE2 and test if the provided WTM user's identity is valid.
If the WTM user's identity is valid then test if the WTM user is authorised for the service.
If the WTM user is authorised for the service then send AP-ENQ-request to FE6.
If the WTM user is not authorised for the service then send AU-PARM-response (rejected) to FE2.
If the WTM user's identity is invalid then send AU-PARM-response (rejected) to FE2.

502 Receive AP-ENQ-confirm (accepted) from FE6 and send AU-PARM-response (accepted) to FE2.

503 Receive AP-ENQ-confirm (rejected) from FE6 and send AU-PARM-response (rejected) to FE2.

8.3.6 Functional entity actions of FE6

601 Receive AP-ENQ-indication from FE5 requesting authentication parameters stored and test if available.
If available then retrieve it and test if computation of a challenge and expected response is required.
If required then compute the challenge and expected response and send AP-ENQ-response (accepted) to FE5.
If not required then forward the parameters to FE5 in AP-ENQ-response (accepted).
If not available then send AP-ENQ-response (rejected) to FE5.

8.4 Functional entity behaviour

The FE behaviours shown below are intended to illustrate typical FE behaviour in terms of information flows sent and received.

The behaviour of each FE is shown using the Specification and Description Language (SDL) defined in ITU-T Rec. Z.100. Anotations indicate the source of input signals and the destination of output signals, respectively.

8.4.1 Behaviour of FE1

Figure 9 shows the normal behaviour of FE1.

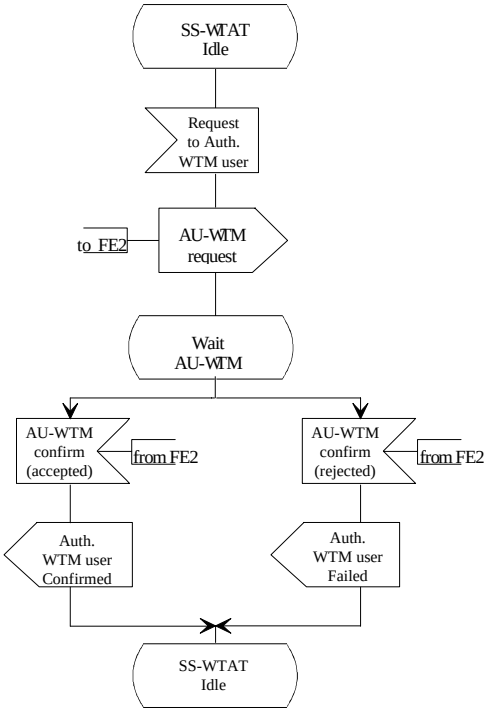

Figure 9: SS-WTAT, SDL for functional entity FE1

8.4.2 Behaviour of FE2

Figure 10 shows the normal behaviour of FE2.

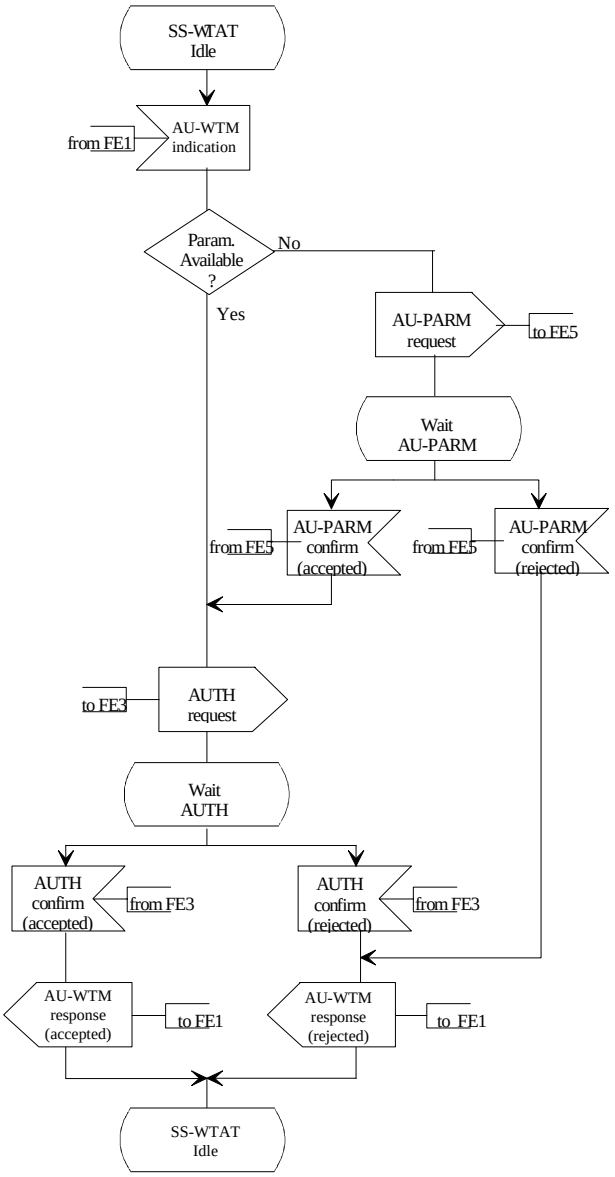

Figure 10: SS-WTAT, SDL for functional entity FE2

8.4.3 Behaviour of FE3

Figure 11 shows the normal behaviour of FE3.

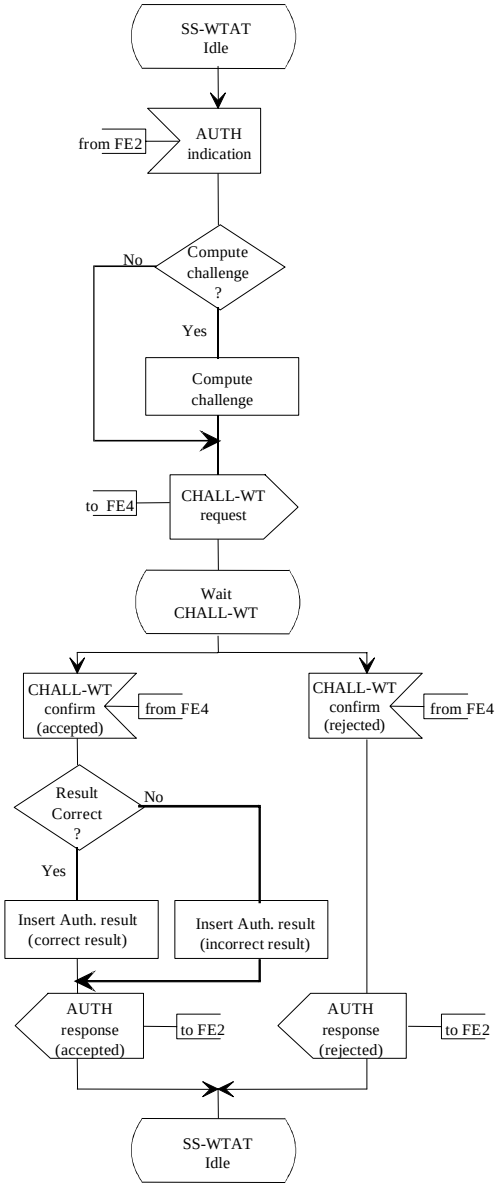

Figure 11: SS-WTAT, SDL for functional entity FE3

8.4.4 Behaviour of FE4

Figure 12 shows the normal behaviour of FE4.

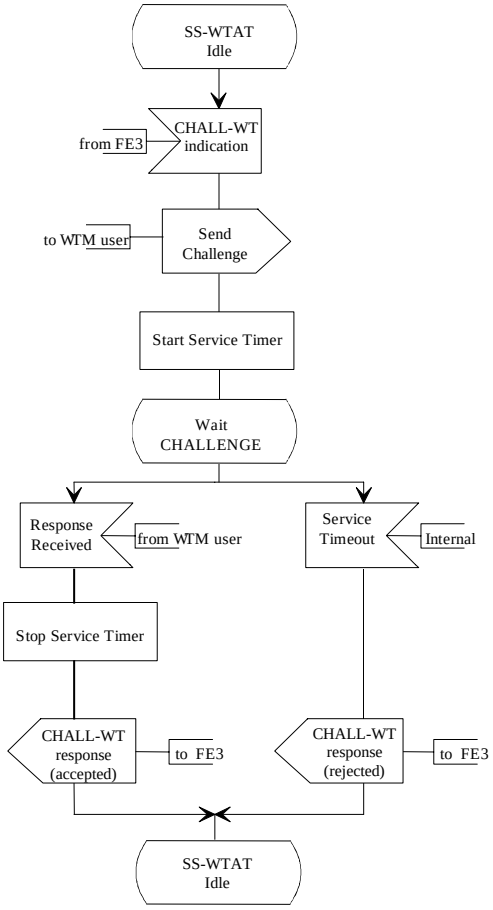

Figure 12: SS-WTAT, SDL for functional entity FE4

8.4.5 Behaviour of FE5

Figure 13 shows the normal behaviour of FE5.

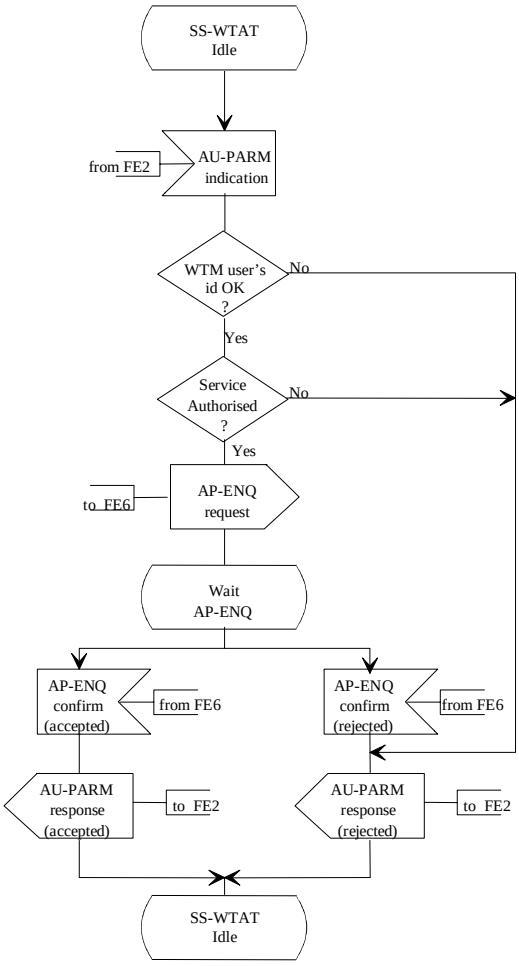

Figure 13: SS-WTAT, SDL for functional entity FE5

8.4.6 Behaviour of FE6

Figure 14 shows the normal behaviour of FE6.

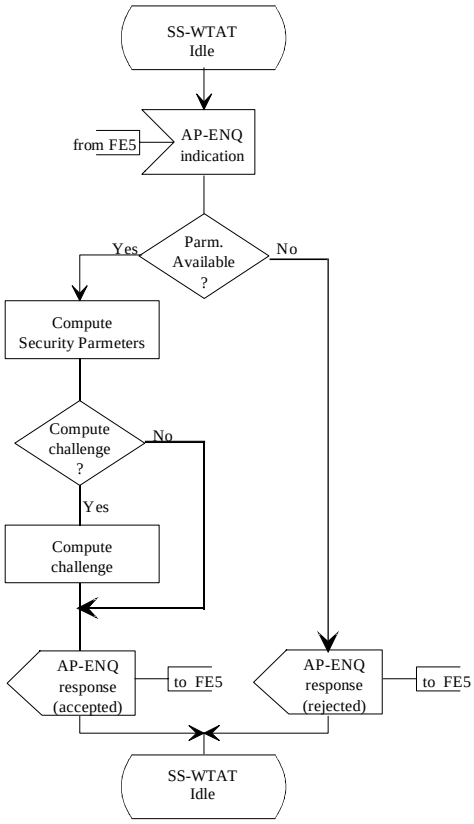

Figure 14: SS-WTAT, SDL for functional entity FE6

8.5 Allocation of functional entities to physical equipment

The allocation of FEs to physical location is shown in Table 6.

Table 6: Scenarios for the allocation of FEs to physical equipment

	FE1	FE2	FE3	FE4	FE5	FE6
Scenario 1	Visitor PINX	Visitor PINX	FP	FP	Home PINX	Auth. Server
Scenario 2	Visitor PINX	Visitor PINX	Visitor PINX	FP	Home PINX	Auth. Server
Scenario 3	Visitor PINX	Visitor PINX	Visitor PINX	Visitor PINX	Home PINX	Auth. Server
Scenario 4	FP	Visitor PINX	FP	FP	Home PINX	Auth. Server
Scenario 5	FP	Visitor PINX	Visitor PINX	FP	Home PINX	Auth. Server
Scenario 6	Home PINX	Visitor PINX	FP	FP	Home PINX	Auth Server
Scenario 7	Home PINX	Visitor PINX	Visitor PINX	FP	Home PINX	Auth Server
Scenario 8	Home PINX	Visitor PINX	Visitor PINX	Visitor PINX	Home PINX	Auth. Server
Scenario 9	Home PINX	Home PINX	Visitor PINX	FP	Home PINX	Auth. Server
Scenario 10	Home PINX	Home PINX	Visitor PINX	Visitor PINX	Home PINX	Auth. Server
Scenario 11	Home PINX	Home PINX	Home PINX	FP	Home PINX	Auth. Server
Scenario 12	Home PINX	Home PINX	Home PINX	Visitor PINX	Home PINX	Auth. Server

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

8.6 Interworking considerations

Not applicable.

9 SS-WTAN stage 2 specification

9.1 Functional model

9.1.1 Functional model description

The functional model shall comprise the following functional entities:

FE1: WTM served user agent
FE2: Authentication execution
FE3: Authentication control
FE4 Home location control
FE5 Authentication centre

The following functional relationships shall exist between these functional entities:

rx between FE1 and FE2
ry between FE2 and FE3
rz between FE3 and FE4
rw between FE4 and FE5

Figure 15 shows these FEs and relationships.

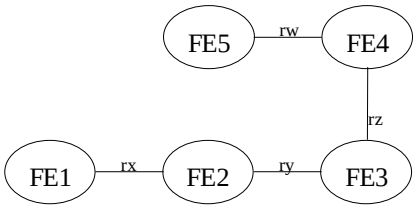

Figure 15: Functional model for SS-WTAN

9.1.2 Description of functional entities

9.1.2.1 WTM served user agent, FE1

If requested by the WTM user, this entity forwards any challenge provided by the WTM user to FE2 and returns any received response to the WTM user.

9.1.2.2 Authentication execution, FE2

This entity receives a challenge from FE1, computes a response and returns it to FE1. If this entity has insufficient parameters to calculate the response, it requests them from FE3.

9.1.2.3 Authentication control, FE3

This entity requests authentication parameters if needed, from FE4 upon a request from FE2.

9.1.2.4 Home location, FE4

This FE requests authentication parameters from FE5, on request from FE3.

9.1.2.5 Authentication centre, FE5

This FE provides FE4 with authentication parameters related to a WTM user on request from FE4.

9.1.3 Relationship of functional model to basic call functional model

All information flows are independent of basic call flows.

9.2 Information flows

9.2.1 Definition of information flows

In the tables listing the service elements in information flows, the column headed "Request" indicates which of these service elements are mandatory (M) and which are optional (O) in a request/indication information flow, and the column headed "Confirm" indicates which of these service elements are mandatory (M) and which are optional (O) in a response/confirmation information flow.

9.2.1.1 AP-ENQ

AP-ENQ is a confirmed information flow across rw from FE4 to FE5 which requests FE5 to provide authentication parameters of a WTM user.

Table 7 lists the service elements within the AP-ENQ information flow.

Table 7: Content of AP-ENQ

Service Elements	Allowed Values	Request	Confirm
WTM user's identity		M	
Authentication Service	SS-WTAN	M	
Challenge		O	
Authentication Algorithm	Algorithm identification	O	
Computation possible	Yes/No	O	
Result	Accepted/Rejected		M
Authentication Parameters			O (note 1)
Cause of rejection	Parameters not available		O (note 2)

NOTE 1: The authentication parameters shall be provided if the request is accepted.

NOTE 2: This service element may be included only if the service is rejected.

NOTE The Authentication parameters in AP-ENQ confirm contain either a set of parameters sufficient to compute a response by another FE or the response itself.

9.2.1.2 AU-PARM

AU-PARM is a confirmed information flow across rz from FE3 to FE4 which requests FE4 to provide authentication parameters of a WTM user.

Table 4 lists the service elements within the AU-PARM information flow.

Table 8: Content of AU-PARM

Service Elements	Allowed Values	Request	Confirm
WTM user's identity		M	
Authentication Service	SS-WTAN	M	
Challenge		O	
Authentication Algorithm	Algorithm identification	O	
Computation possible	Yes/No	O	
Result	Accepted/Rejected		M
Authentication Parameters			O (note 1)
Cause of rejection	WTM user unknown WTM user not authorised for SS-WTAN Parameters not available		O (note 2)

NOTE 1: The authentication parameters shall be provided if the request is accepted

NOTE 2: This service element may be included only if the service is rejected.

NOTE The Authentication parameters in AU-PARM confirm contain either a set of parameters sufficient to compute a response by another FE or the response itself.

9.2.1.3 CHALL-PISN

CHALL-PISN is a confirmed information flow across rx from FE1 to FE2 which indicates to FE2 that a challenge has been received from FE1 and it shall provide a response.

Table 9 lists the service elements within the CHALL-PISN information flow.

Table 9: Content of CHALL-PISN

Service Elements	Allowed Values	Request	Confirm
WTM user's identity		M	
Challenge		M	
Result	Accept/Reject		M
Response value			O (note 1)
Cause of rejection	WTM user not authorised for SS-WTAN SS-WTAN not supported		O (note 2)

NOTE 1: The Response value service element shall be included if the service is accepted.

NOTE 2: This service element may be included only if the service is rejected.

9.2.1.4 RETRIEVE

RETRIEVE is a confirmed information flow across ry from FE2 to FE3 which requests FE3 to forward authentication parameters to FE2.

Table 10 lists the service elements within the RETRIEVE information flow.

Table 10: Content of RETRIEVE

Service Elements	Allowed Values	Request	Confirm
WTM user's identity		M	
Challenge		O	
Authentication Algorithm	Algorithm identification	O	
Computation possible	Yes/No	O	
Result	Accepted/Rejected		M
Authentication Parameters			O(note 1)
Cause of rejection	WTM user unknown Parameters not available		O (note 2)

NOTE 1: The authentication parameters shall be provided if the request is accepted.

NOTE 2: This service element may be included only if the service is rejected.

NOTE The Authentication parameters in RETRIEVE confirm contain either a set of parameters sufficient to compute a response by another FE or the response itself.

9.2.2 Relationship of information flows to basic call information flows

All information flows are independent of basic call flows.

9.2.3 Examples of information flow sequences

A stage 3 International Standard for SS-WTAN shall provide signalling procedures in support of the information flow sequences specified below. In addition, signalling procedures should be provided to cover other sequences arising from error situations, interactions with basic call, interactions with other supplementary services, different topologies, etc.

In the figures, SS-WTAN information flows are represented by solid arrows and basic call information flows are represented by broken arrows. An ellipse embracing two information flows indicates that the two information flows occur simultaneously. Within a column representing an SS-WTAN functional entity, the numbers refer to functional entity actions listed in 8.3. The following abbreviations are used:

req request

ind indication

resp response

conf confirmation

9.2.3.1 Successful authentication of a PISN (parameters available locally in FE2)

Figure 16 shows the information for successful authentication of a PISN with parameters being locally available FE2.

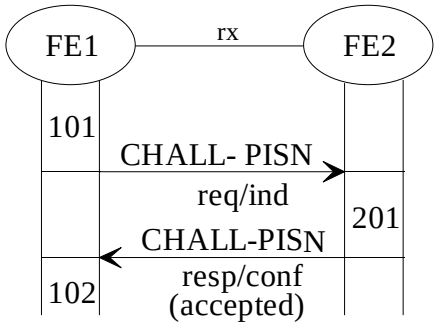

Figure 16: Successful case with parameters available locally in FE2

9.2.3.2 Successful authentication of a PISN (parameters retrieved by FE3)

Figure 17 shows the information flow for successful authentication of a PISN with the parameters being retrieved from FE4 by FE3.

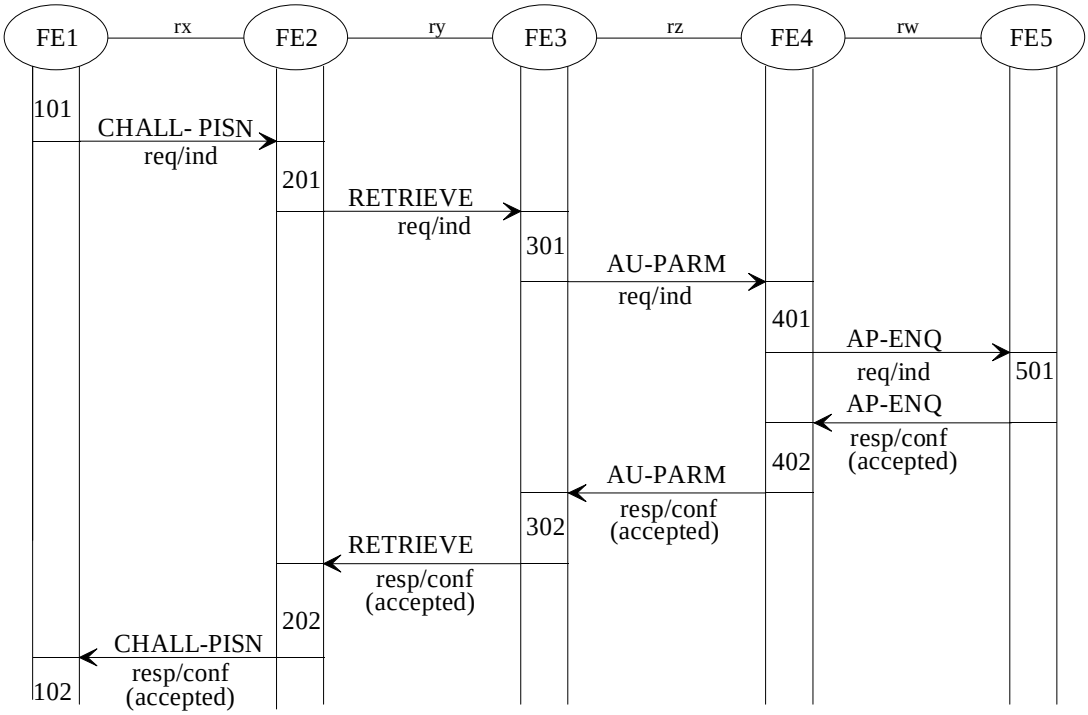

Figure 17: Successful case with parameters retrieved from FE5 by FE2

9.2.3.3 Unsuccessful authentication of a PISN (rejection from FE5)

Figure 18 shows the information flow for unsuccessful authentication of a PISN where a rejection is received from FE2 due to unsuccessful parameter retrieval.

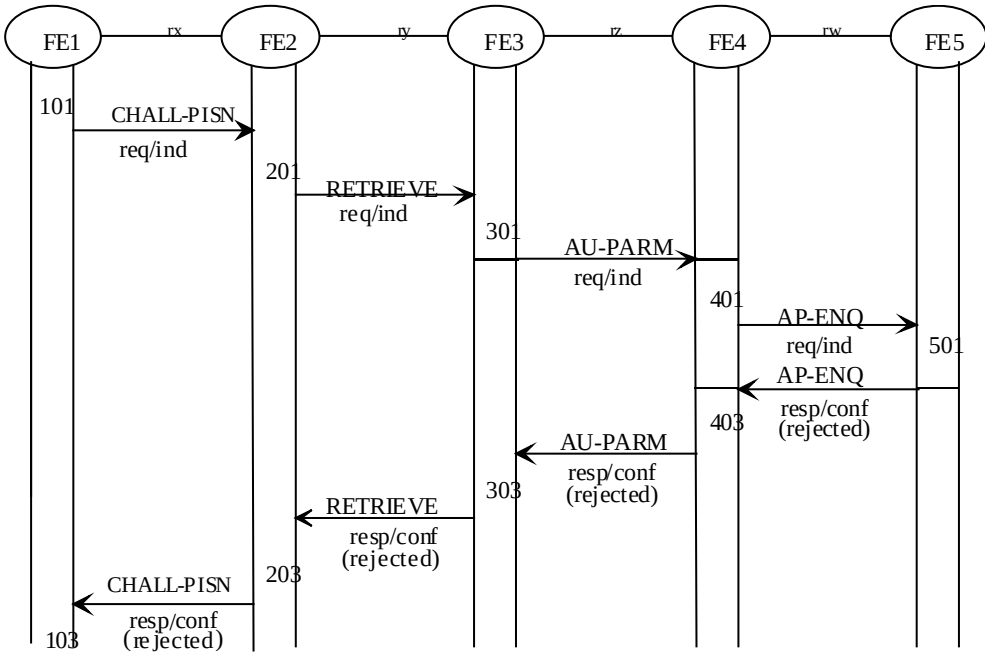

Figure 18: Unsuccessful case, rejection from FE4

9.3 Functional entity actions

The following FE actions shall occur at the points indicated in the figures of 8.2.3.

9.3.1 Functional entity actions of FE1

101 Receive an indication to authenticate the PISN and send CHALL-PISN-request to FE2.

102 Receive CHALL-PISN-confirm (accepted) from FE2 and send response (accepted) to the WTM user.

103 Receive CHALL-PISN-confirm (rejected) from FE2 and send response (rejected) to the WTM user

9.3.2 Functional entity actions of FE2

201 Receive CHALL-PISN-indication and test if parameters are locally available.
If they are available then compute a response and send CHALL-PISN-response (accepted) to FE1.
If the parameters are not available then send RETRIEVE-request to FE3.

202 Receive RETRIEVE-confirm (accepted) from FE3 and test if a response needs to be computed.
If required then compute a response and send CHALL-PISN-response (accepted) to FE1.
If not required then forward the received response to FE1 in CHALL-PISN-response (accepted).

203 Receive RETRIEVE-confirm (rejected) from FE3. Send CHALL-PISN-response (rejected) to FE1

9.3.3 Functional entity actions of FE3

301 Receive RETRIEVE-indication from FE2 and test if parameters are available locally.
If the parameters are available locally then send RETRIEVE-response (accepted) to FE2.
If the parameters are not available locally then send AU-PARM-request to FE4.

302 Receive AU-PARM-confirm (accepted) from FE4 and send RETRIEVE-response (accepted) to FE2

303 Receive AU-PARM-confirm (rejected) from FE4 and send RETRIEVE-response (rejected) to FE2.

9.3.4 Functional entity actions of FE4

401 Receive AU-PARM-indication from FE3 and test if the provided WTM user's identity is valid.
If the WTM user's identity is valid then test if the WTM user is authorised for the service.

If the WTM user is authorised for the service then send AP-ENQ-request to FE5.
If the WTM user is not authorised for the service then send AU-PARM-response (rejected) to FE3.
If the WTM user's identity is invalid then send AU-PARM-response (rejected) to FE3.

402 Receive AP-ENQ-confirm (accepted) from FE5 and send AU-PARM-response (accepted) to FE3.

403 Receive AP-ENQ-confirm (rejected) from FE5 and send AU-PARM-response (rejected) to FE3.

9.3.5 Functional entity actions of FE5

501 Receive AP-ENQ-indication from FE4 requesting authentication parameters stored and test if available.
If available then retrieve it and test if required to compute a response.
If required then compute response and send AP-ENQ-response (accepted) to FE4.
If not required then send parameters to FE4 in AP-ENQ-response (accepted).
If not available then send AP-ENQ-response (rejected) to FE4.

9.4 Functional entity behaviour

The FE behaviours shown below are intended to illustrate typical FE behaviour in terms of information flows sent and received.

The behaviour of each FE is shown using the Specification and Description Language (SDL) defined in ITU-T Rec. Z.100. Anotations indicate the source of input signals and the destination of output signals, respectively.

9.4.1 Behaviour of FE1

Figure 19 shows the normal behaviour of FE1.

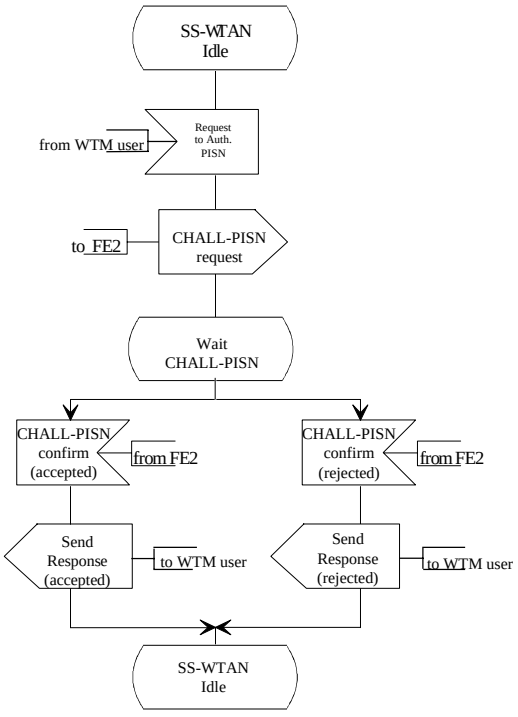

Figure 19: SS-WTAN, SDL for functional entity FE1

9.4.2 Behaviour of FE2

Figure 20 shows the normal behaviour of FE2.

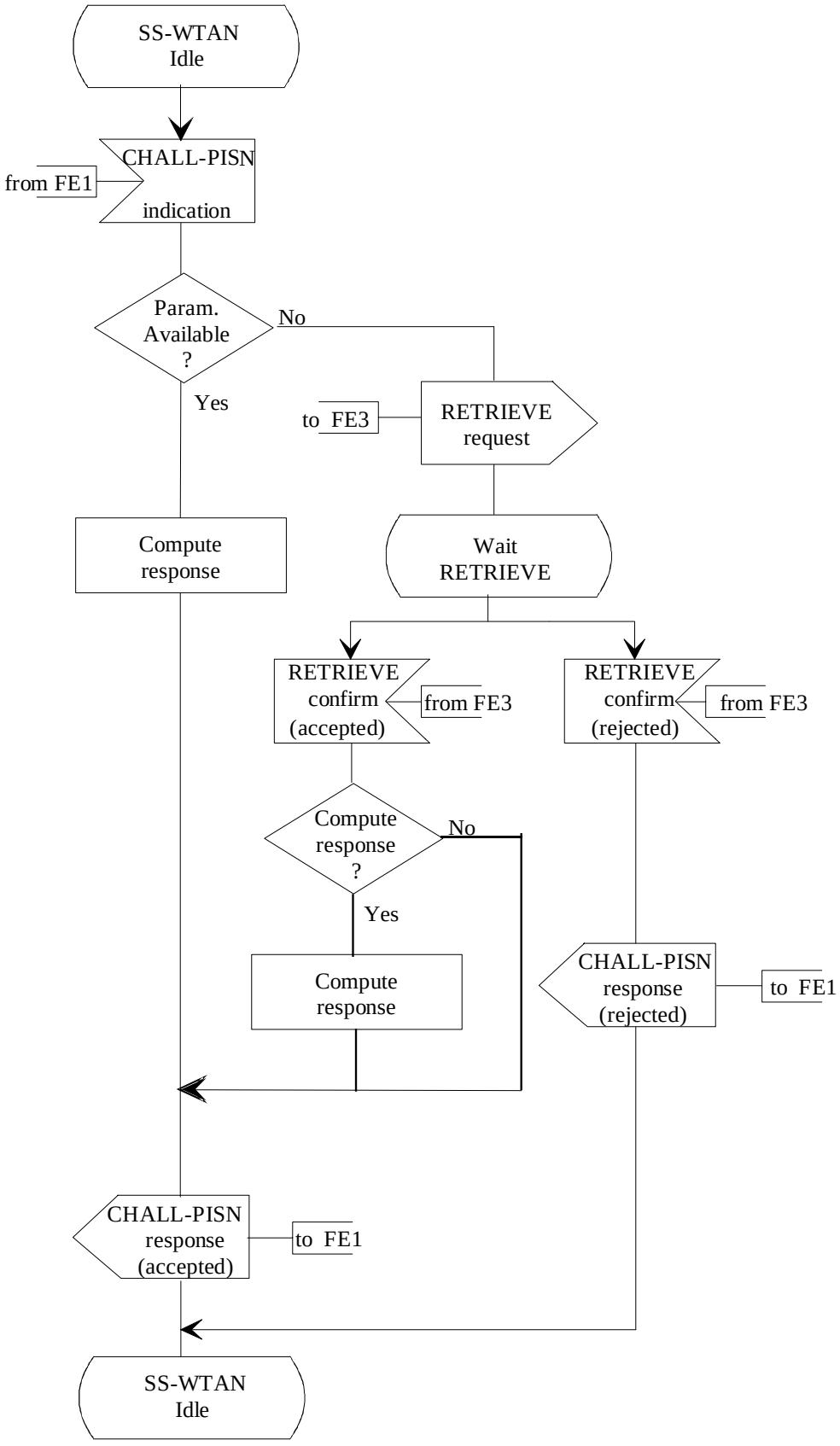

Figure 20: SS-WTAN, SDL for functional entity FE2

9.4.3 Behaviour of FE3

Figure 21 shows the normal behaviour of FE3.

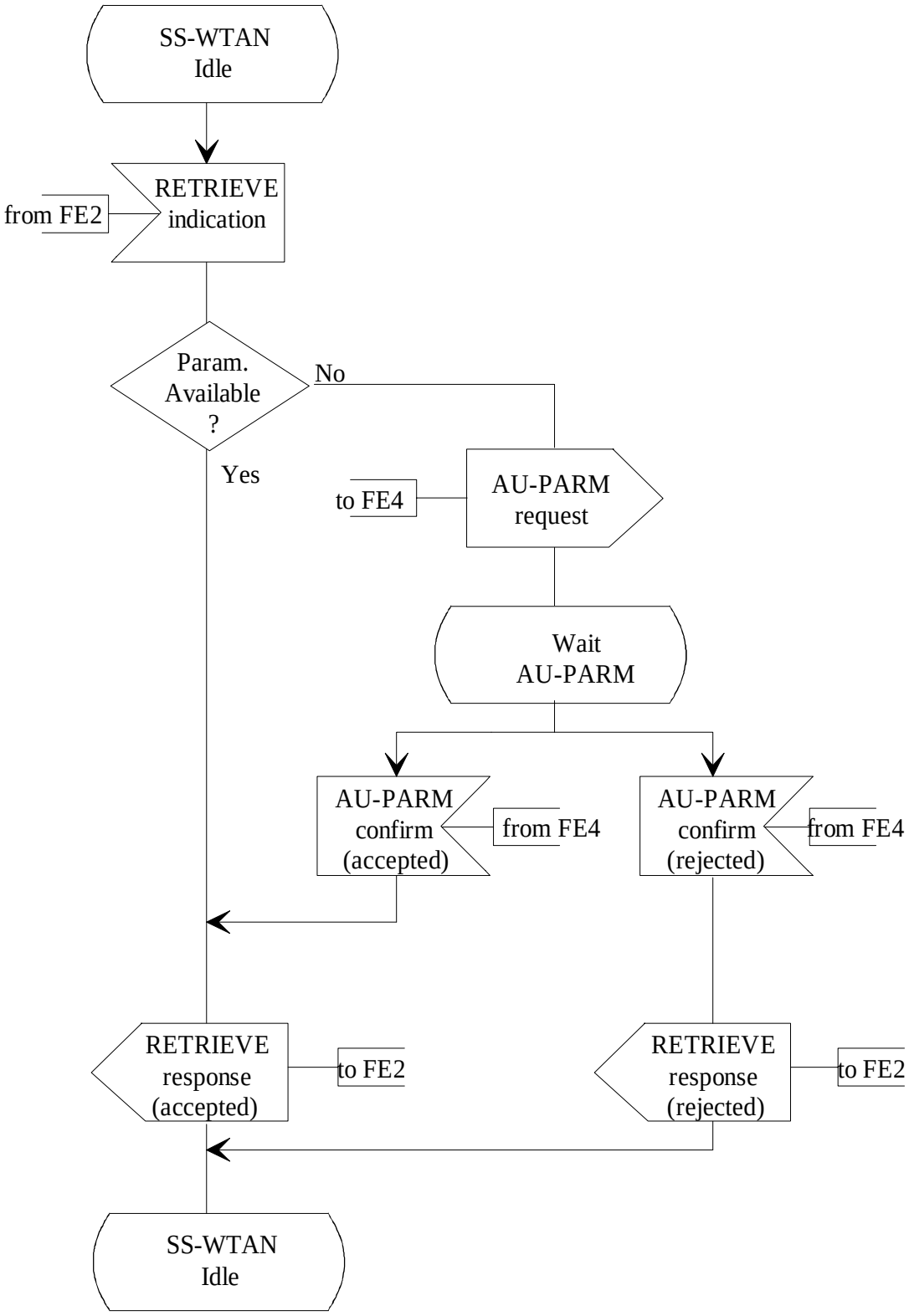

Figure 21: SS-WTAN, SDL for functional entity FE3

9.4.4 Behaviour of FE4

Figure 22 shows the normal behaviour of FE4.

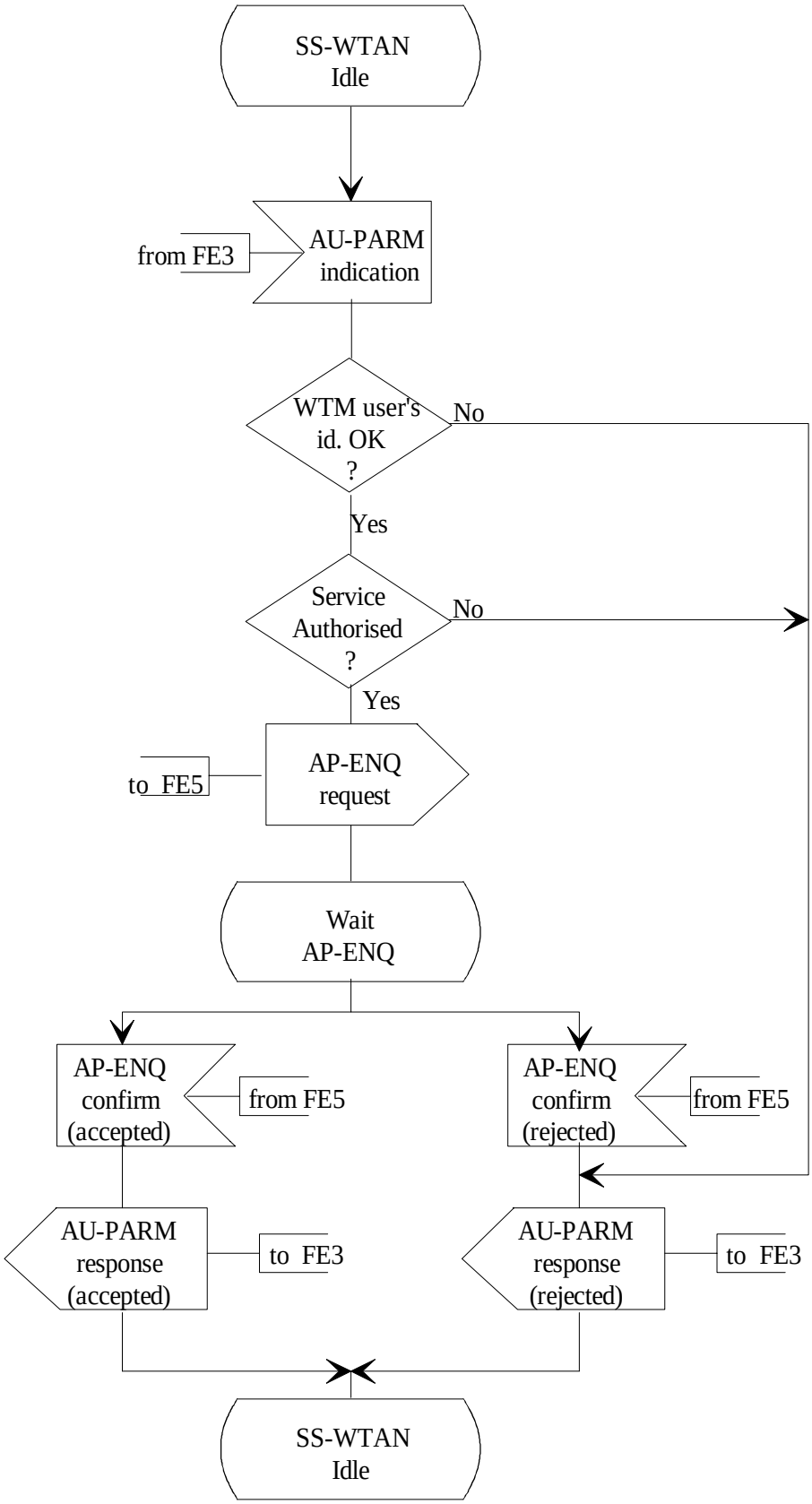

Figure 22: SS-WTAN, SDL for functional entity FE4

9.4.5 Behaviour of FE5

Figure 23 shows the normal behaviour of FE5.

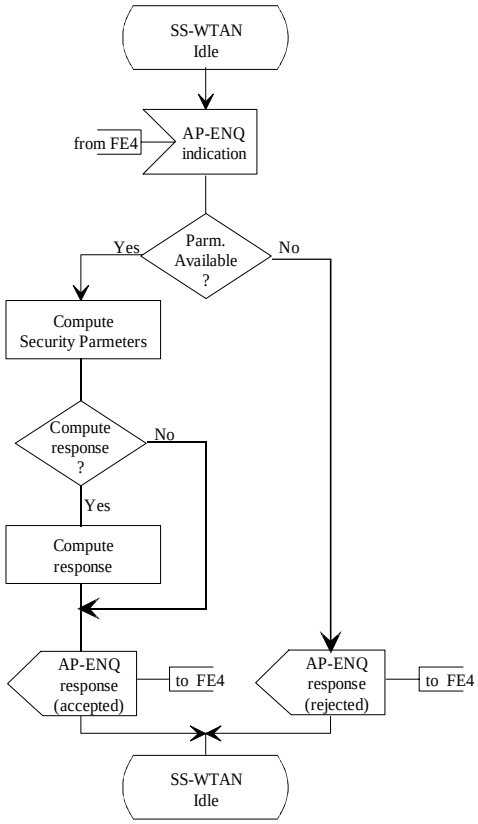

Figure 23: SS-WTAN, SDL for functional entity FE5

9.5 Allocation of functional entities to physical equipment

The allocation of FEs to physical location is shown in Table 11.

Table 11: Scenarios for the allocation of FEs to physical equipment

	FE1	FE2	FE3	FE4	FE5
Scenario 1	FP	FP	Visitor PINX	Home PINX	Auth. Server
Scenario 2	FP	Visitor PINX	Visitor PINX	Home PINX	Auth. Server
Scenario 3	Visitor PINX	Visitor PINX	Visitor PINX	Home PINX	Auth. Server
Scenario 4	FP	FP	Home PINX	Home PINX	Auth. Server
Scenario 5	FP	Visitor PINX	Home PINX	Home PINX	Auth. Server
Scenario 6	Visitor PINX	Visitor PINX	Home PINX	Home PINX	Auth. Server
Scenario 7	FP	Home PINX	Home PINX	Home PINX	Auth. Server
Scenario 8	Visitor PINX	Home PINX	Home PINX	Home PINX	Auth. Server

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

9.6 Interworking considerations

Not applicable.

Annex A
(informative)
User identifiers

A.1 WTM user's identity

The WTM user's identity is referred to throughout this standard and is considered to have four possible forms:

a) a PISN number as defined in ISO/IEC 11571;

b) a permanent identity equivalent to the PISN number and which is understood for the identification of the WTM user at the Home PINX and partly at the Visitor PINX. This identity can be used throughout the PISN to determine the location of the WTM user's HDB;

c) a permanent identifier which has no immediate meaning to the PISN. This may be the only one available for terminals that do not allow the network operator to enter an identity into the terminal. A directory service is required to translate such an identifier into a PISN number;

d) a temporary identity which is partly understood at each Visitor PINX, and fully understood by the old Visitor PINX where it can be translated into the PISN number. A temporary identity can be used instead of the permanent identity as a security measure such that the user's permanent identity is not transmitted across the air interface. A network assigned identity (NAI) or an equivalent identity may be used.

ICS 33.040.35

Price based on 34 pages