INTERIM EUROPEAN TELECOMMUNICATION STANDARD

FINAL DRAFT
pr **I-ETS 300 769**

April 1997

Source: ETSI TC-BTC

Reference: DI/BTC-01038

ICS: 33.020

Key words: CTM, mobility, PISN, supplementary service, stage 2

Private Integrated Services Network (PISN); Cordless Terminal Mobility (CTM); Authentication; Functional capabilities and information flows

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 4 92 94 42 00 - Fax: +33 4 93 65 47 16

Contents

Foreword

This final draft Interim European Telecommunication Standard (I-ETS) has been produced by the Business TeleCommunications (BTC) Technical Committee of the European Telecommunications Standards Institute (ETSI), and is now submitted to for the Voting phase of the ETSI standards approval procedure.

An ETSI standard may be given I-ETS status either because it is regarded as a provisional solution ahead of a more advanced standard, or because it is immature and requires a "trial period". The life of an I-ETS is limited to three years after which it can be converted into an ETS, have its life extended for a further two years, be replaced by a new version, or be withdrawn.

Proposed announcement date	
Date of latest announcement of this I-ETS (doa):	3 months after ETSI publication

Blank page

1 Scope

This Interim European Telecommunication Standard (I-ETS) describes the stage two of the Authentication services for Private Telecommunication Networks (PISNs). It comprises two related but distinct service descriptions. The first is a supplementary service allowing a PISN to authenticate a Cordless Terminal Mobility (CTM) user. It is called Supplementary Service - Cordless Terminal Authentication of the Terminal (SS-CTAT). The second is a service whereby a CTM user may authenticate the PISN. It is called Supplementary Service - Cordless Terminal Authentication of the Network (SS-CTAN). Stage 2 identifies the functional entities involved in the feature and the information flows between them.

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

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

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

Authentication algorithms to be used by these two supplementary services (SS-CTAT and SS-CTAN) are outside the scope of this I-ETS. This I-ETS provides the information flows to convey the security parameters within the PISN.

Supplementary service specifications are produced in three stages according to the method specified in ETS 300 387 [1]. This I-ETS contains stage 2 specification of the authentication supplementary services.

The purpose of stage 2 specification is to guide and constrain the work on signalling protocols at stage 3, while fulfilling the requirements of stage 1 ETS 300 768 [3]. Stage 1 and stage 3 are defined in separate I-ETSs.

This I-ETS applies to CTM only within a single PISN. The specification of information flows between the PISN and cordless terminals is beyond the scope of this I-ETS.

2 Conformance

Conformance to this I-ETS is met by conforming to a stage three standard which fulfils the requirements of this I-ETS that are relevant to the equipment for which the stage three standard applies. Therefore no method of testing is provided for this I-ETS.

3 Normative references

This I-ETS incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] ETS 300 387 (1994): "Private telecommunication network (PTN) - Method for the specification of basic and supplementary services".

[2] ETS 300 171 (1992): "Private telecommunication network (PTN) - Specification, functional model and information flows - Control aspects of circuit mode basic services".

[3] ETS 300 768 (1996): "Private Integrated Services Network (PISN) - Cordless Terminal Mobility (CTM) - Authentication Service description".

[4] CCITT Recommendation Z.100 (1988): "Functional specification and description language (SDL)".

[5] ETS 300 691 (1996): "Private Integrated Service Network (PISN) Cordless Terminal Mobility (CTM); Location handling services; service description".

[6] CCITT Recommendation I.210 (1988): "Principles of telecommunication services supported by an ISDN and means to describe them".

[7] ETS 300 415 (1996): "Private Integrated Services Network (PISN) - Terms and definitions".

[8] ETS 300 695 (1996): "Private Integrated Services Network (PISN); Cordless Terminal Mobility (CTM); Call handling additional network features; Functional capabilities and information flows".

4 Definitions

For the purposes of this I-ETS, the following definitions apply:

Additional Network Feature: A capability over and above that of a basic service, provided by a PISN, but not directly to a PISN user.

authentication: See ETS 300 415 [7].

authentication server: The PINX that contains the functionality to compute a challenge for a CTM user.

Cordless Terminal Mobility: See ETS 300 691 [5].

Cordless Terminal Mobility User: For the purpose of this I-ETS, CTM user is defined as the user being authenticated by SS-CTAT or the authenticating user of SS-CTAN.

Fixed Part: See ETS 300 695 [8].

home PINX: The PINX which has direct access to the HDB entry for a particular CTM user.

PISN authority: The body or its representative responsible for arranging the service with the service provider.

PISN user: See ETS 300 691 [5].

visitor PINX: The PINX that is serving a CTM user at a visited area.

Supplementary Service: See CCITT Recommendation I.210 [6] paragraph 2.4.

5 Abbreviations

For the purposes of this I-ETS, the following abbreviations apply:

ANF	Additional Network Feature
CT	Cordless Terminal
CTM	Cordless Terminal Mobility
FP	Fixed Part
PISN	Private Integrated Service Network
PTN	Private Telecommunication Network
SS	Supplementary Service
SS-CTAT	Supplementary Service - Authentication of a CTM user
SS-CTAN	Supplementary Service - Authentication of a PISN

6 SS-CTAT

6.1 Description

Authentication of a Cordless Terminal user (CTAT) enables the PISN, as a security measure, to validate the identity provided by the CTM user. This is done by sending specific information to the CTM user and awaiting a response. If the response is not the expected response, the PISN shall be informed and can then take any action as appropriate.

6.2 Functional model

6.2.1 Functional model description

The functional model for the SS-CTAT supplementary service shall be as shown in figure 1.

The figure shows the different Functional Entities (FE) and their relationship with other entities.

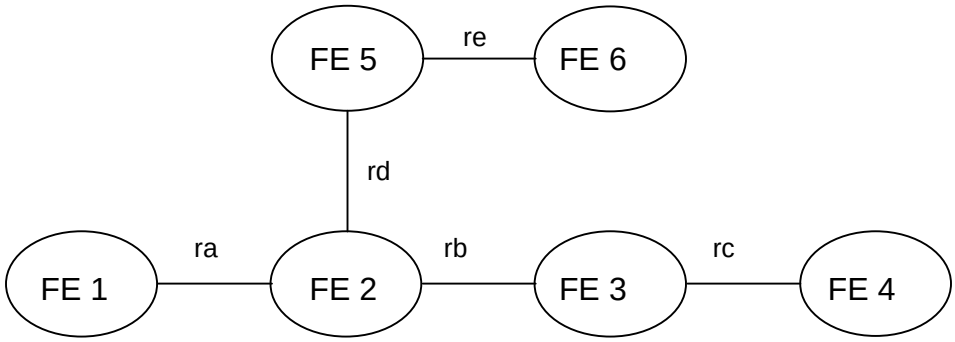


Figure 1: Functional model for SS-CTAT

The functional model shall comprise the following entities:

FE1: CTAT initiator
FE2: Authentication detection and control
FE3: Authentication execution
FE4: CTM 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

6.2.2 Description of functional entities

6.2.2.1 CTAT initiator, FE1

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

6.2.2.2 Authentication detection and control, FE2

This FE detects a request for authentication from FE1 and requests the necessary parameters, if needed, from FE5. It then requests FE3 to execute the authentication of the specified CTM user.

6.2.2.3 Authentication execution, FE3

This FE receives the request to authenticate a CTM user. It computes a challenge and an expected response, if these have not been provided by FE6. It receives responses to the challenges from FE4.

6.2.2.4 CTM served user agent, FE4

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

6.2.2.5 Home location, FE5

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

6.2.2.6 Authentication centre, FE6

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

6.2.3 Relationship with basic service

All information flows are independent of basic call information flows.

6.3 Information flows

6.3.1 Information flow diagrams

6.3.1.1 Successful authentication of a CTM user (parameters available locally)

Figure 2 shows the information flow for successful authentication of a CTM user with parameters being available locally in FE2.

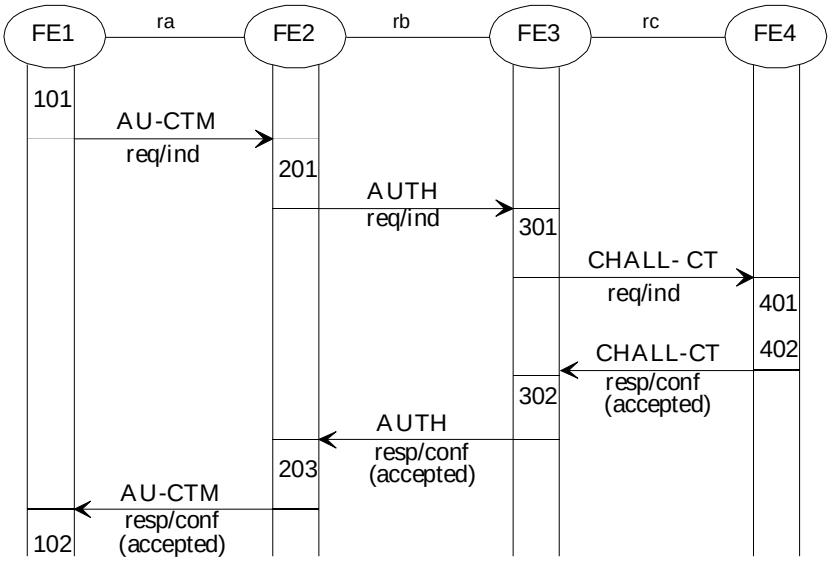


Figure 2: Successful case with parameters available locally in FE2

6.3.1.2 Successful authentication of a CTM user (parameters retrieved from FE5)

Figure 3 shows the information flow for successful authentication of a CTM user. The authentication parameters are retrieved from FE5 by FE2 prior to continuing with the authentication.

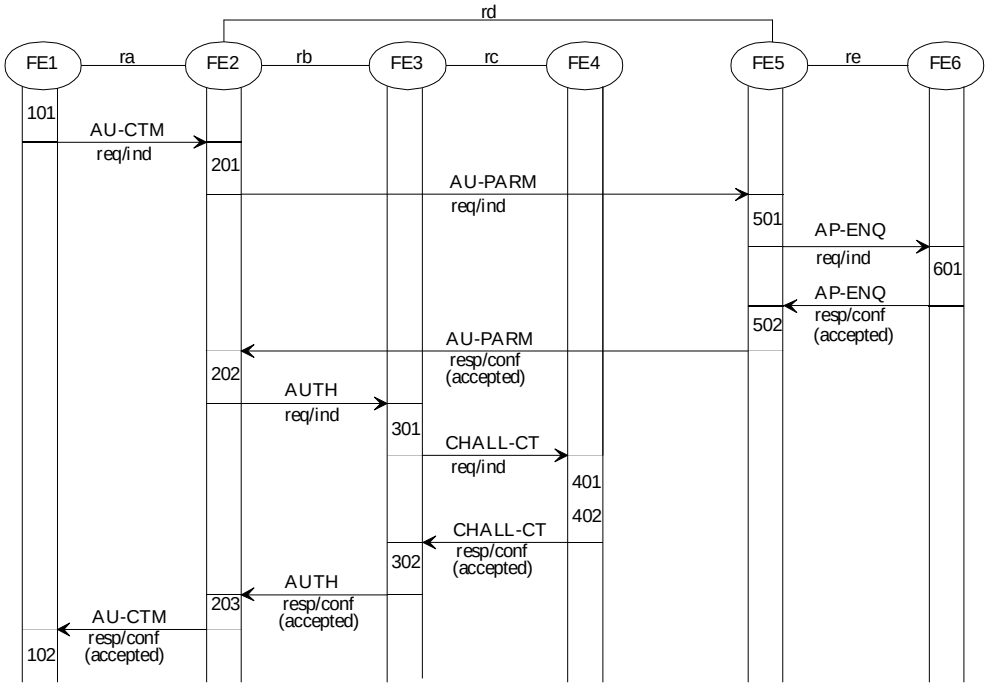
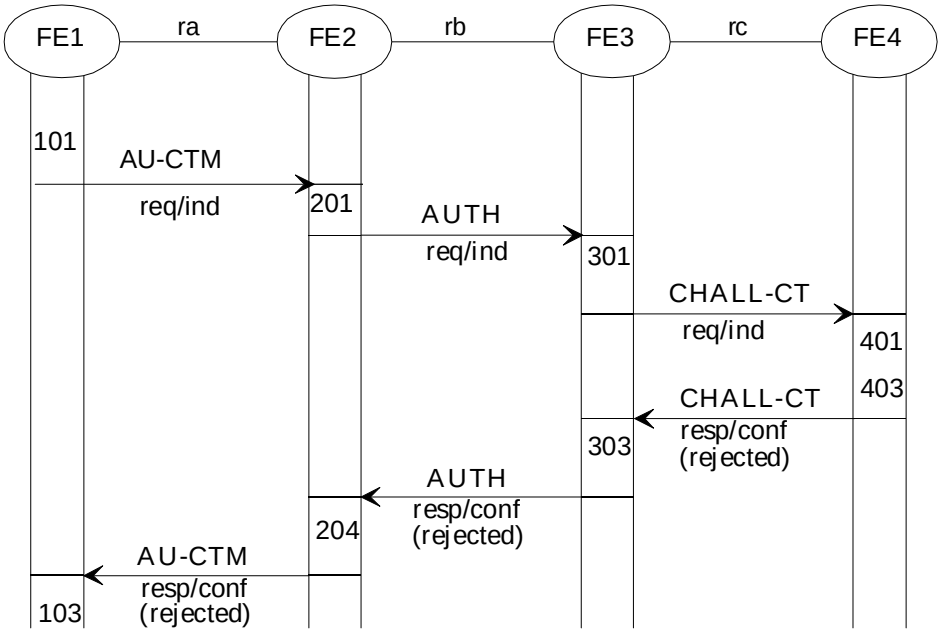


Figure 3: Successful case with parameters retrieved from FE5 by FE2

6.3.1.3 Unsuccessful authentication of a CTM user (rejection from FE4)

Figure 4 shows the information flow for unsuccessful authentication of a CTM user where a rejection is received from FE4 (e.g. CT not accessible or an internal service time out).



NOTE: This example assumes the parameters are available locally at FE2.

Figure 4: Unsuccessful case, rejection from FE4.

6.3.1.4 Unsuccessful authentication of a CTM user (parameter retrieval rejection from FE5)

Figure 5 shows the information flow for unsuccessful authentication of a CTM user where a rejection is received from FE5 (e.g. incorrect CTM user's identity).

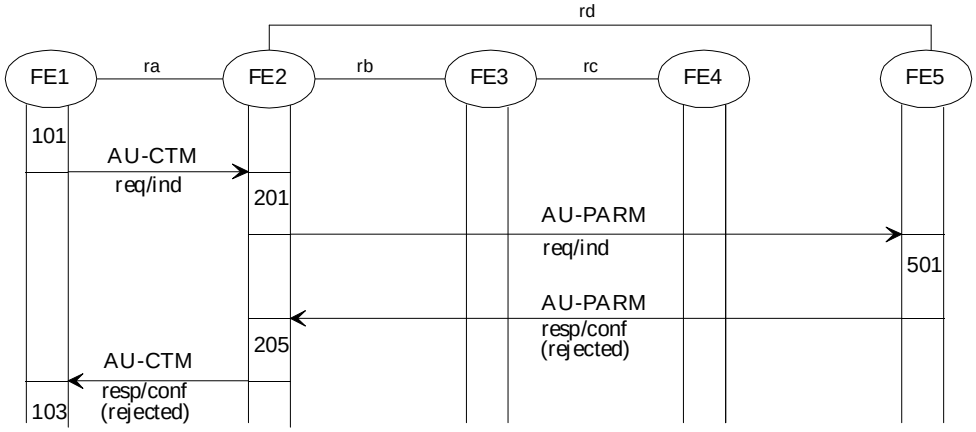


Figure 5: Unsuccessful case, rejection from FE5

6.3.1.5 Unsuccessful authentication of a CTM user (parameter retrieval rejection from FE6)

Figure 6 shows the information flow for unsuccessful authentication of a CTM user where a rejection is received from FE6 (e.g. parameters not available).

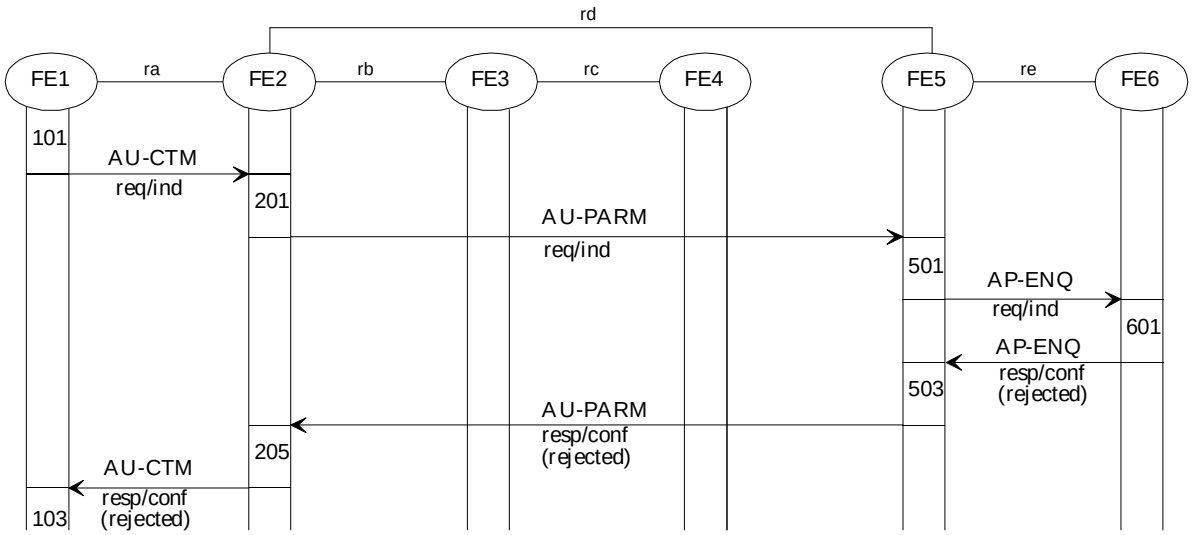


Figure 6: Unsuccessful case, rejection from FE6

6.3.2 Definition of individual information flows

6.3.2.1 AP-ENQ

This confirmed information flow requests FE6 to provide authentication parameters of a CTM user. It shall be sent across relationship re, from FE5 to FE6 and shall contain the following service elements.

Table 1: Contents of AP-ENQ

Service Elements	Allowed Values	Request	Confirm
CTM user's identity	note 1	M	
Authentication Service	SS-CTAT	M	
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 CTM 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.

6.3.2.2 AU-CTM

This confirmed information flow conveys a request to authenticate a CTM user. It shall be sent across relationship ra, from FE1 to FE2 and shall contain the following service elements.

Table 2: AU-CTM

Service Elements	Allowed Values	Request	Confirm
CTM user's identity		M	
Result	Accept/Reject		M
Accept Result	CT auth result correct		O (note 1)
	CT auth result incorrect		
Cause of rejection	CT 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.			

6.3.2.3 AU-PARM

This confirmed information flow requests FE5 to provide authentication parameters of a CTM user. It shall be sent across relationship rd, from FE2 to FE5 and it shall contain the following service elements.

Table 3: Contents of AU-PARM

Service Elements	**Allowed Values**	**Request**	**Confirm**
CTM user's identity		M	
Authentication Service	SS-CTAT	M	
Result	Accepted/Rejected		M
Authentication Parameters			O (note 1)
Cause of rejection	CTM user unknown		O (note 2)
	CTM user not authorized for SS-CTAT		
	Parameters not available		
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.

6.3.2.4 AUTH

This confirmed information flow requests FE3 to authenticate the CTM user. It shall be sent across relationship rb, from FE2 to FE3 and it shall contain the following service elements.

Table 4: Contents of AUTH

Service Elements	**Allowed Values**	**Request**	**Confirm**
CTM user's identity		M	
Authentication Parameters		M	
Result	Accept/Reject		M
Accept result	CT auth result correct		O (note 1)
	CT auth result incorrect		
Cause of rejection	CT 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 either a set of parameters sufficient to compute a challenge and/or response by another FE or both a challenge and expected response.

6.3.2.5 CHALL-CT

This confirmed information flow indicates to FE4 that it shall forward the challenge to the CTM user. The information flow shall be sent across relationship rc, from FE3 to FE4 and shall contain the following service elements.

Table 5: Contents of CHALL-CT

Service Elements	Allowed Values	Request	Confirm
CTM user's identity		M	
Challenge		M	
Result	Accept/Reject		M
Response value			O (note 1)
Cause of rejection	CT 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.			

6.4 SDL diagrams for functional entities

The figures in this subclause are intended to illustrate typical FE behaviour in terms of information flows sent and received. The behaviour of each FE is shown using SDL diagrams as defined in CCITT Recommendation Z.100 [4].

The direction of each input and output (left or right) corresponds to the direction of messages in the flow diagrams. With the exception of internal events, each input is tagged with the origination FE and each output is tagged with the destination FE.

6.4.1 Behaviour of FE1

Figure 7 shows the SDL diagram for the functional entity FE1.

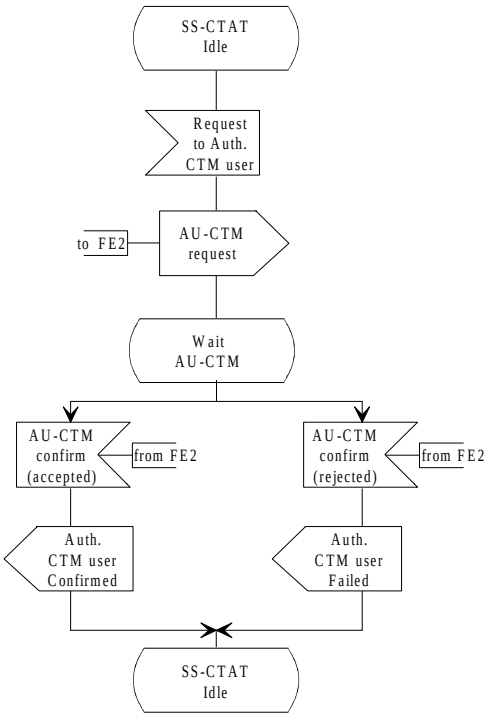


Figure 7: SDL for Functional Entity FE1

6.4.2 Behaviour of FE2

Figure 8 shows the SDL diagram for the functional entity FE2.

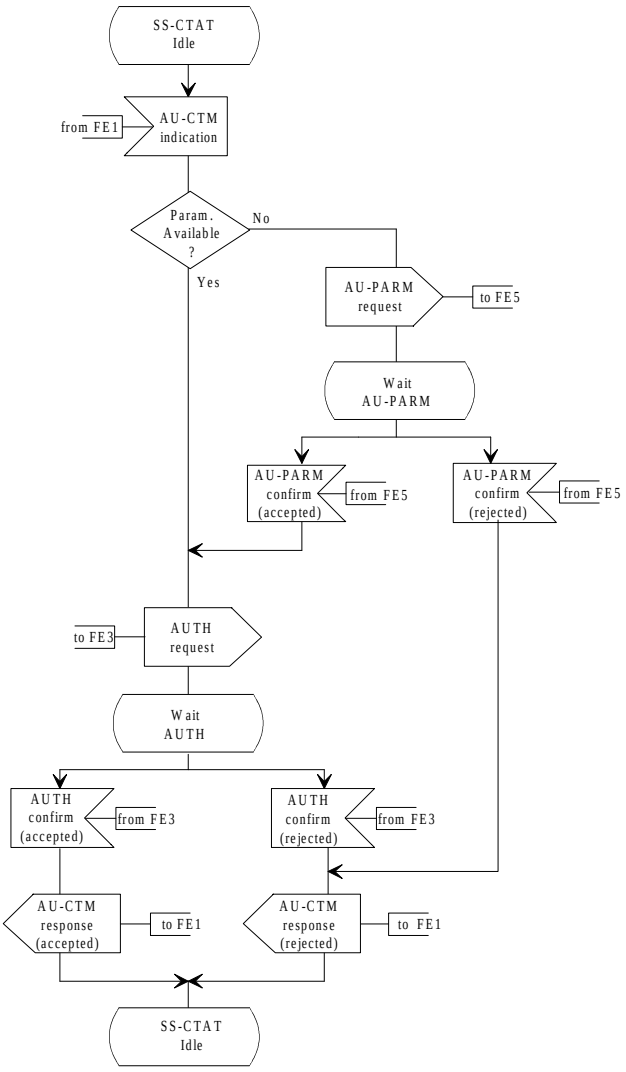


Figure 8: SDL for Functional Entity FE2

6.4.3 Behaviour of FE3

Figure 9 shows the SDL diagram for the functional entity FE3.

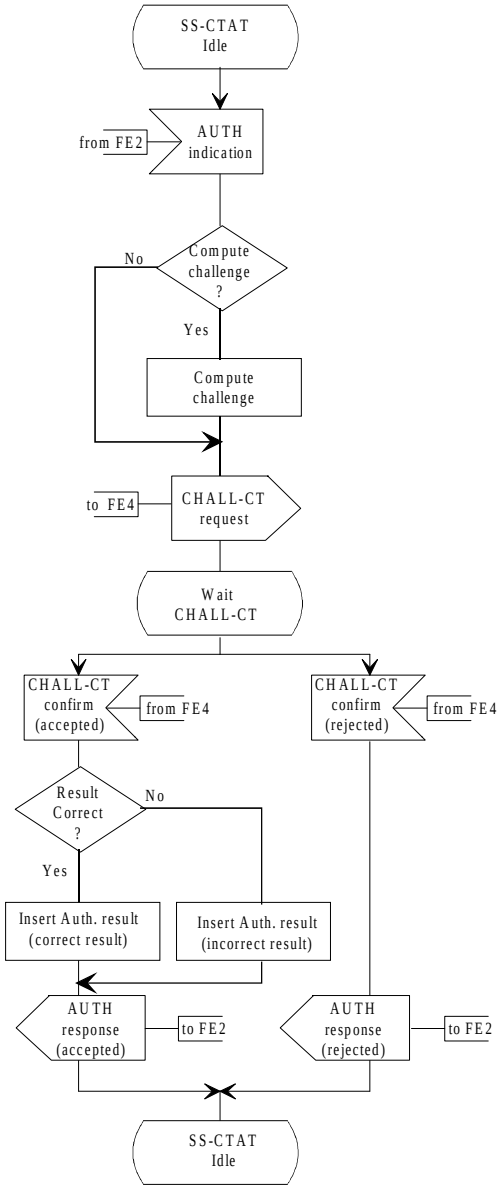


Figure 9: SDL for Functional Entity FE3

6.4.4 Behaviour of FE4

Figure 10 shows the SDL diagram for the functional entity FE4.

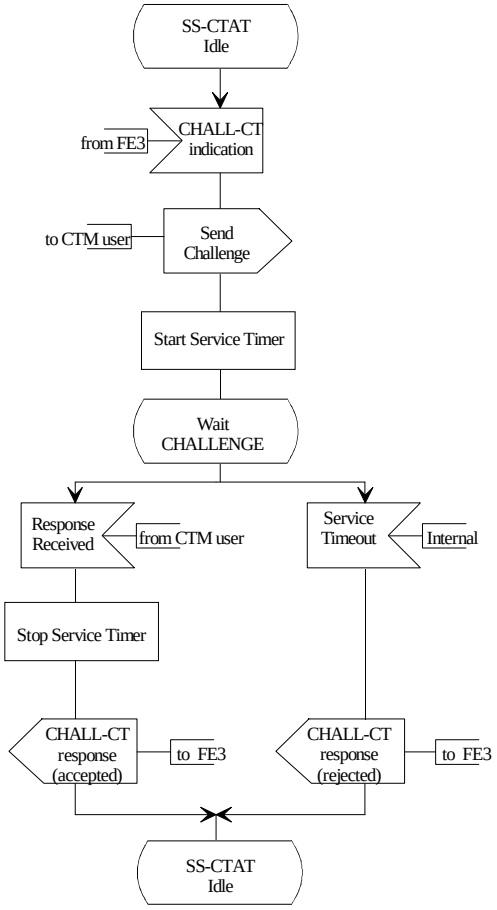


Figure 10: SDL for Functional Entity FE4

6.4.5 Behaviour of FE5

Figure 11 shows the SDL diagram for the functional entity FE5.

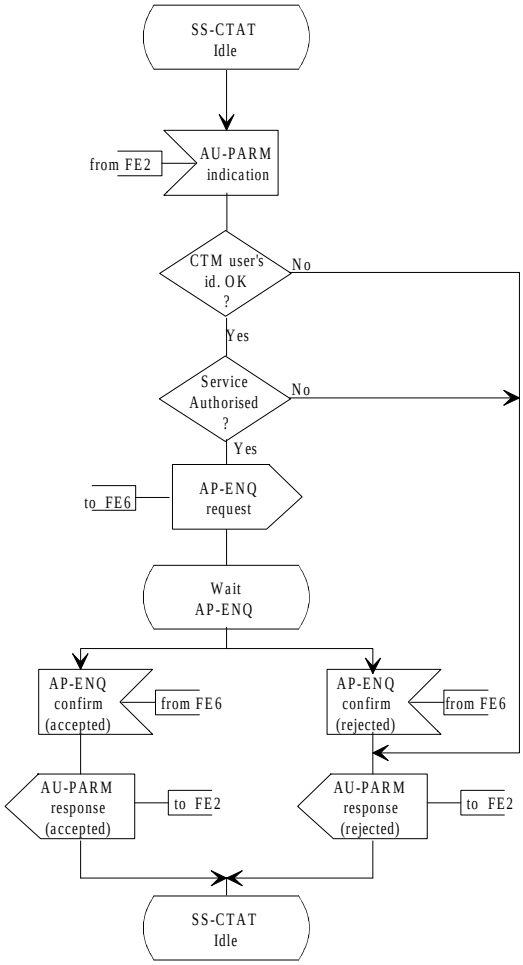


Figure 11: SDL for Functional Entity FE5

6.4.6 Behaviour of FE6

Figure 12 shows the SDL diagram for the functional entity FE6.

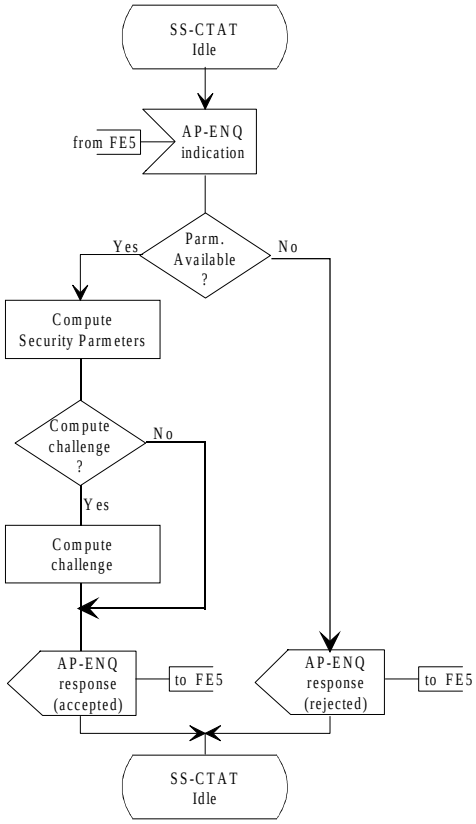


Figure 12: SDL for Functional Entity FE6

6.5 Functional Entity Actions (FEAs)

The following functional entity actions shall take place at the points indicated in the information flow sequences in subclause 6.3.1.

6.5.1 FEAs of FE1

101 Receive a request to authenticate a CTM user, and send AU-CTM-request to FE2.
102 Receive AU-CTM-confirm (accepted) from FE2 and indicate Auth. CTM user confirmed to the initiating entity.
103 Receive AU-CTM-confirm (rejected) from FE2 and indicate Auth. CTM user failed to the initiating entity.

6.5.2 FEAs of FE2

201 Receive AU-CTM-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-CTM-response (accepted) to FE1.
204 Receive AUTH-confirm (rejected) from FE3 and send AU-CTM-response (rejected) to FE1.
205 Receive AU-PARM-confirm (rejected) from FE5 and send AU-CTM-response (rejected) to FE1.

6.5.3 FEAs 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-CT-request to FE4.
If not required then forward the challenge computed by FE6 to FE4 in CHALL-CT-request.

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

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

6.5.4 FEAs of FE4

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

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

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

6.5.5 FEAs of FE5

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

6.5.6 FEAs 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.

6.6 Allocation of functional entities to physical locations

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

Table 6: Allocation of FEs to physical entities.

	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

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

6.7 Interworking Considerations

Not applicable.

7 SS-CTAN

7.1 Description

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

7.2 Functional model

The functional model for the SS-CTAN supplementary service shall be as shown in figure 13.

The figure shows the different functional entities (FE) and their relationship with other entities.

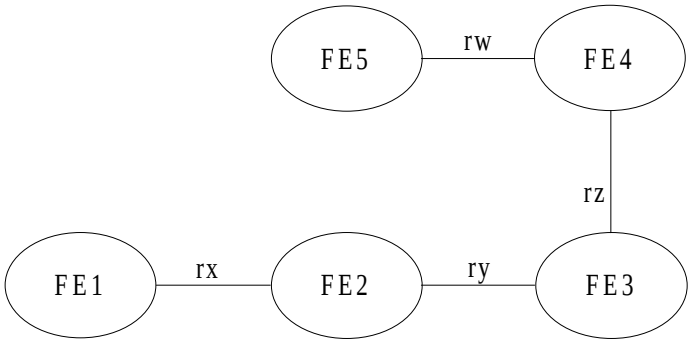


Figure 13: Functional model for SS-CTAN

The functional model shall comprise the following entities:

FE1: CTM 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

7.2.1 Description of functional entities

7.2.1.1 CTM served user agent, FE1

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

7.2.1.2 Authentication execution, FE2

This entity receives a challenge from FE1. It either computes a response and returns it to FE1 or request authentication parameters from FE3.

7.2.1.3 Authentication control, FE3

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

7.2.1.4 Home location, FE4

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

7.2.1.5 Authentication centre, FE5

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

7.2.2 Relationship with basic service

All information flows are independent of basic call information flows.

7.3 Information flows

7.3.1 Information flow diagrams

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

Figure 14 shows the information flow for successful authentication of a PISN with parameters being locally available FE2.

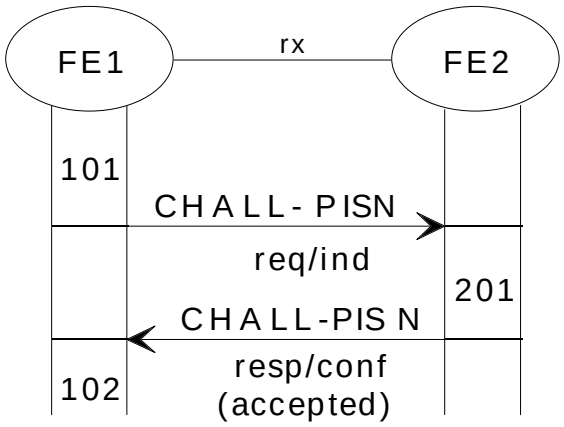


Figure 14: Successful case, parameters available locally in FE2

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

Figure 15 shows the information flow for successful authentication of a PISN with the parameters being retrieved from FE4 by FE3.

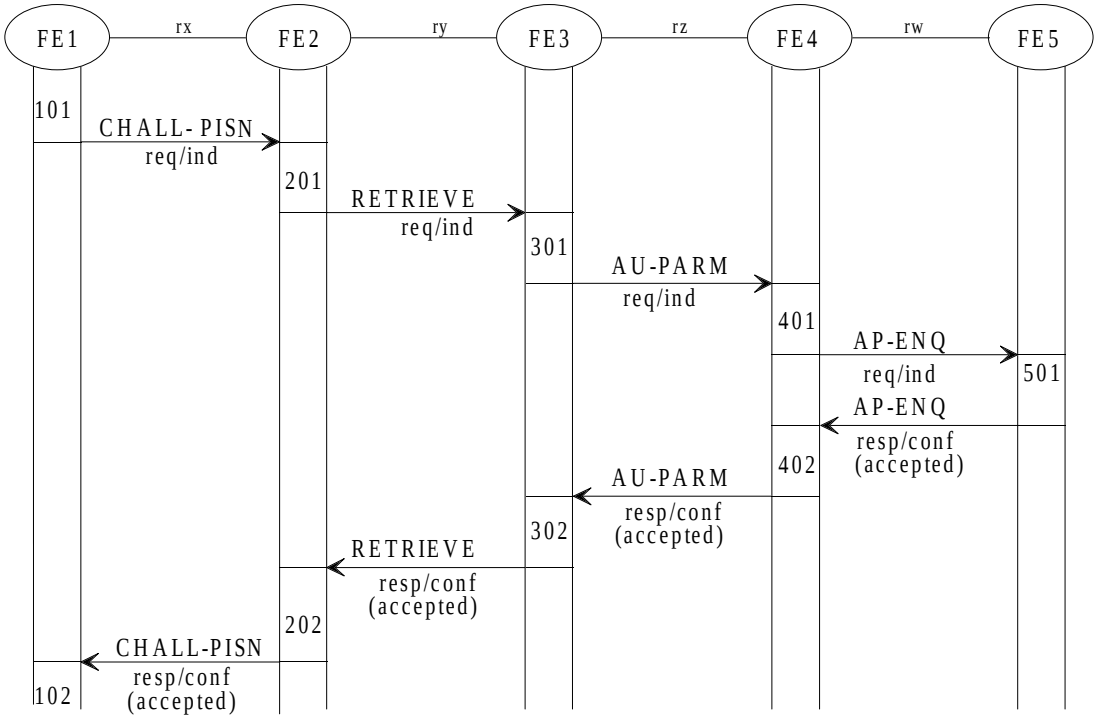


Figure 15: Successful case, parameters retrieved by FE2

7.3.1.3 Unsuccessful authentication of a PISN (rejection from FE5)

Figure 16 shows the information flow for unsuccessful authentication of a PISN where a rejection is received from FE2 due to unsuccessful parameter retrieval.

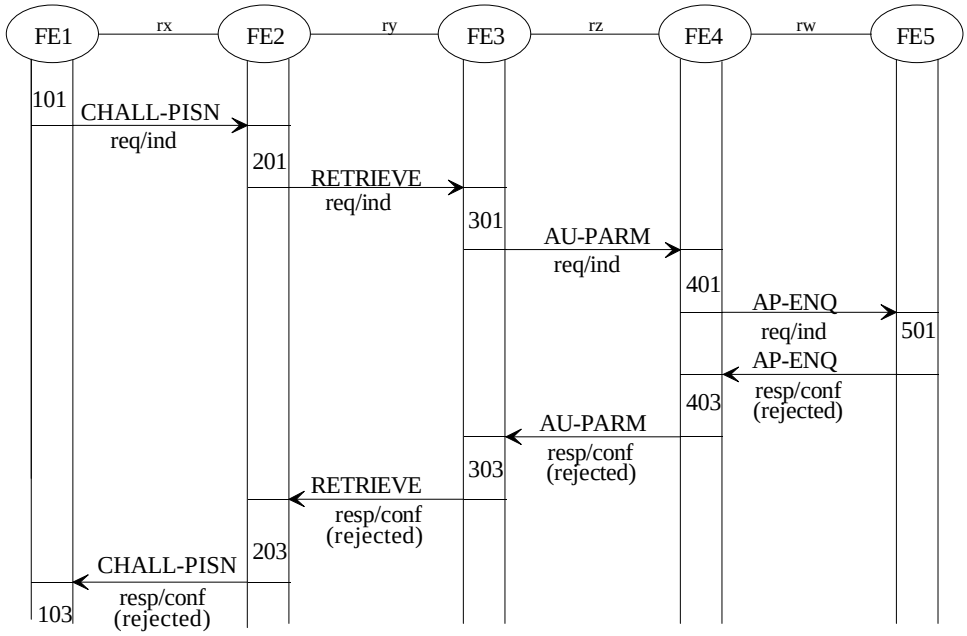


Figure 16: Unsuccessful case, rejection from FE5

7.3.2 Definition of individual information flows

7.3.2.1 AP-ENQ

This confirmed information flow requests FE5 to provide authentication parameters of a CTM user. It shall be sent across relationship rw, from FE4 to FE5 and shall contain the following service elements.

NOTE 1: This information flow is the same as described in subclause 6.3.2.1.

Table 7: Contents of AP-ENQ

Service Elements	Allowed Values	Request	Confirm
CTM user's identity		M	
Authentication Service	SS-CTAN	M	
Challenge		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 2: 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.

7.3.2.2 AU-PARM

This confirmed information flow requests FE4 to provide authentication parameters of a CTM user. It shall be sent across relationship rz, from FE3 to FE4 and shall contain the following service elements.

NOTE 1: This information flow is the same as described in subclause 6.3.2.3.

Table 8: Contents of AU-PARM

Service Elements	Allowed Values	Request	Confirm
CTM user's identity		M	
Authentication Service	SS-CTAN	M	
Challenge		O	
Result	Accepted/Rejected		M
Authentication Parameters			O (note 1)
Cause of rejection	CTM user unknown CTM user not authorized for SS-CTAN 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 2: 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.

7.3.2.3 CHALL-PISN

This confirmed information flow indicates to FE2 that a challenge has been received from FE1 and it shall provide a response. The information flow shall be sent across relationship rx, from FE1 to FE2 and shall contain the following service elements.

Table 9: Contents of CHALL-PISN

Service Elements	Allowed Values	Request	Confirm
CTM user's identity		M	
Challenge		M	
Result	Accept/Reject		M
Response value			O (note 1)
Cause of rejection	CTM user not authorized for SS-CTAN SS-CTAN 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.			

7.3.2.4 RETRIEVE

This confirmed information flow requests FE3 to forward authentication parameters to FE2. It shall be sent across relationship ry, from FE2 to FE3 and shall contain the following information elements.

Table 10: Contents of RETRIEVE

Service Elements	Allowed Values	Request	Confirm
CTM user's identity		M	
Challenge		O	
Result	Accepted/Rejected		M
Authentication Parameters			O(note 1)
Cause of rejection	CTM 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.

7.4 SDL diagrams for functional entities

The figures in this subclause are intended to illustrate typical FE behaviour in terms of information flows sent and received. The behaviour of each FE is shown using SDL diagrams as defined in CCITT Recommendation Z.100 [4].

The direction of each input and output (right or left) corresponds to the direction of messages in the flow diagrams. With the exception of internal events, each input is tagged with the origination FE and each output is tagged with the destination FE.

7.4.1 Behaviour of FE1

Figure 17 shows the SDL diagram for the functional entity FE1.

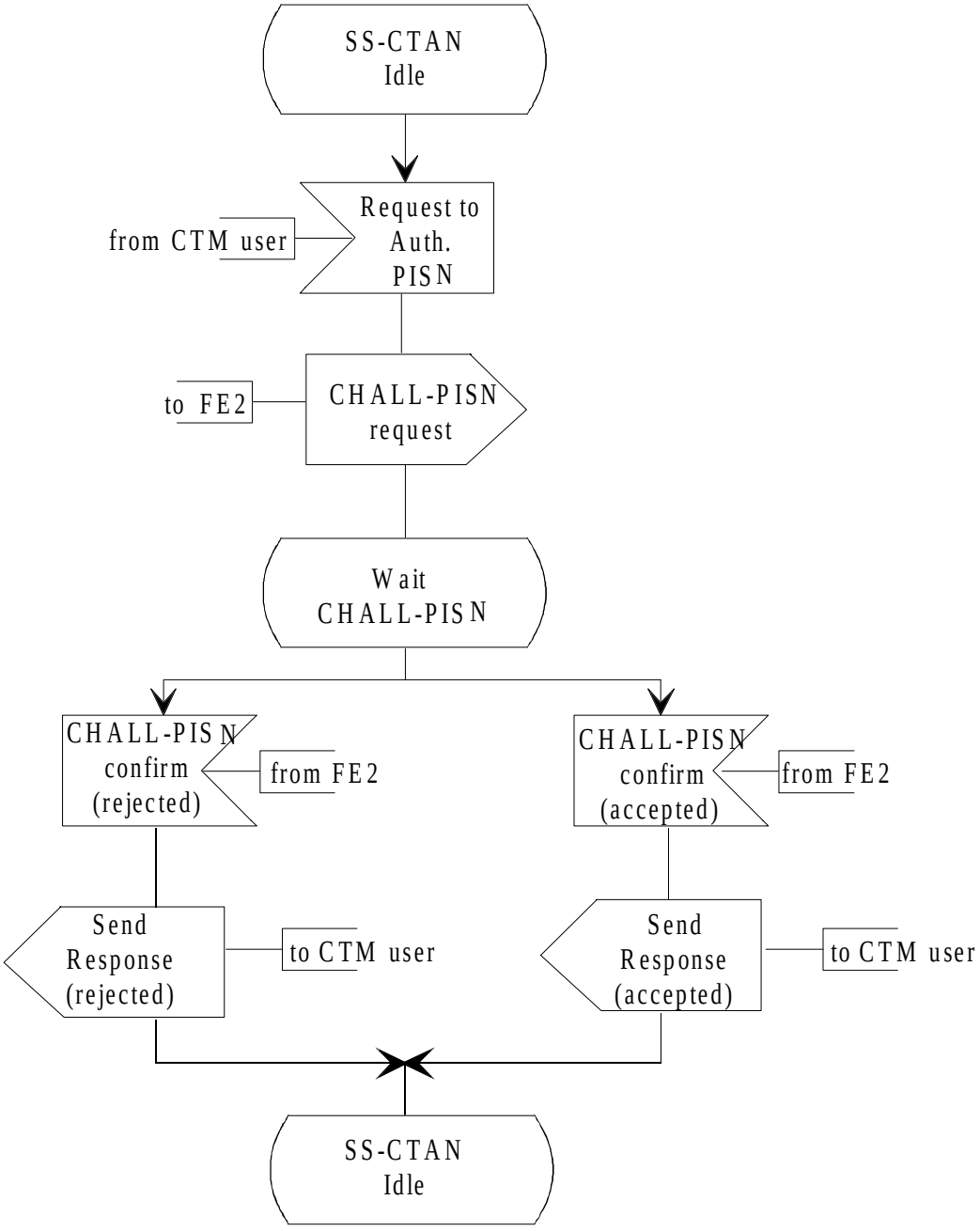


Figure 17: SDL for Functional Entity FE1

7.4.2 Behaviour of FE2

Figure 18 shows the SDL diagram for the functional entity FE2.

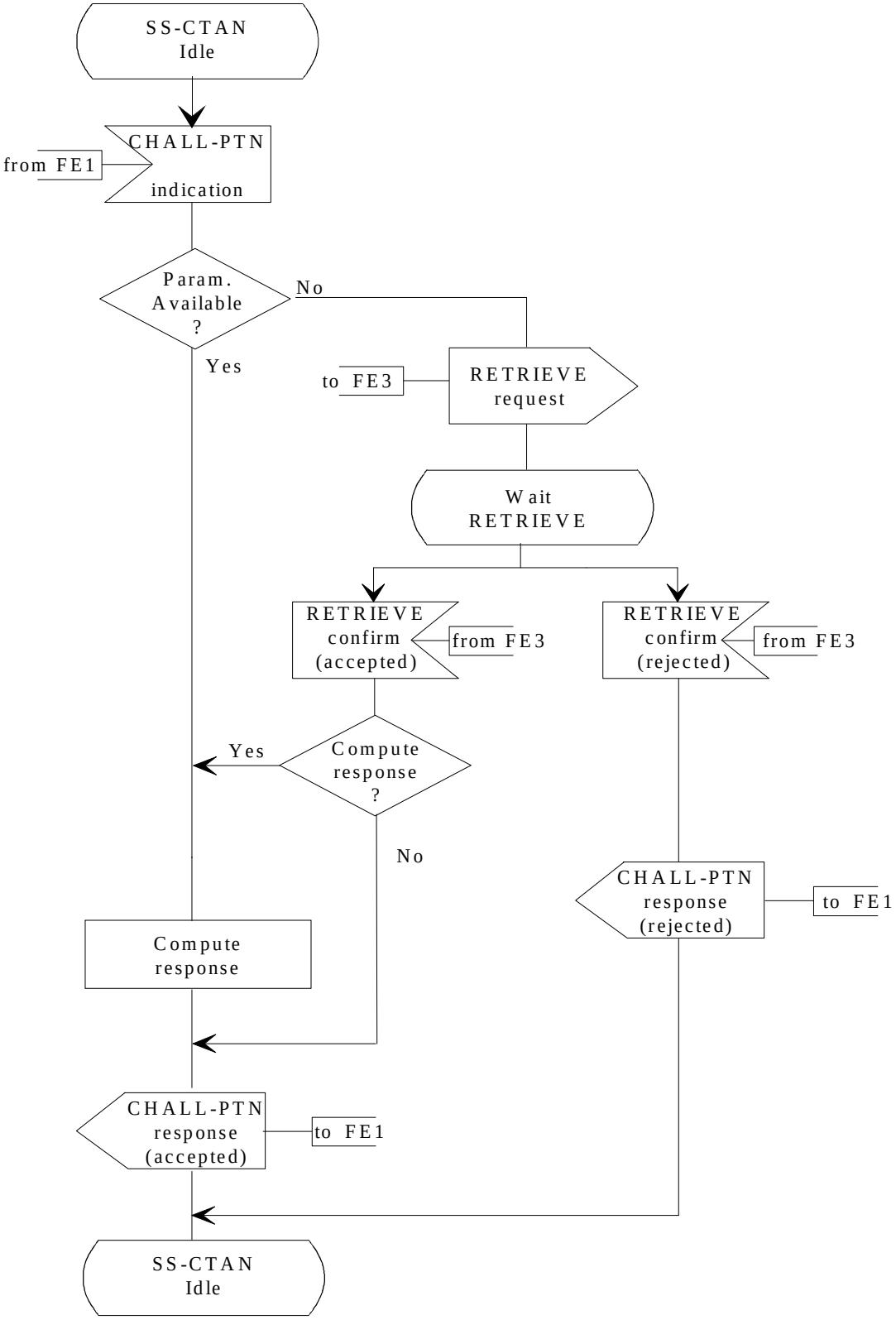


Figure 18: SDL for Functional Entity FE2

7.4.3 Behaviour of FE3

Figure 19 shows the SDL diagram for the functional entity FE3.

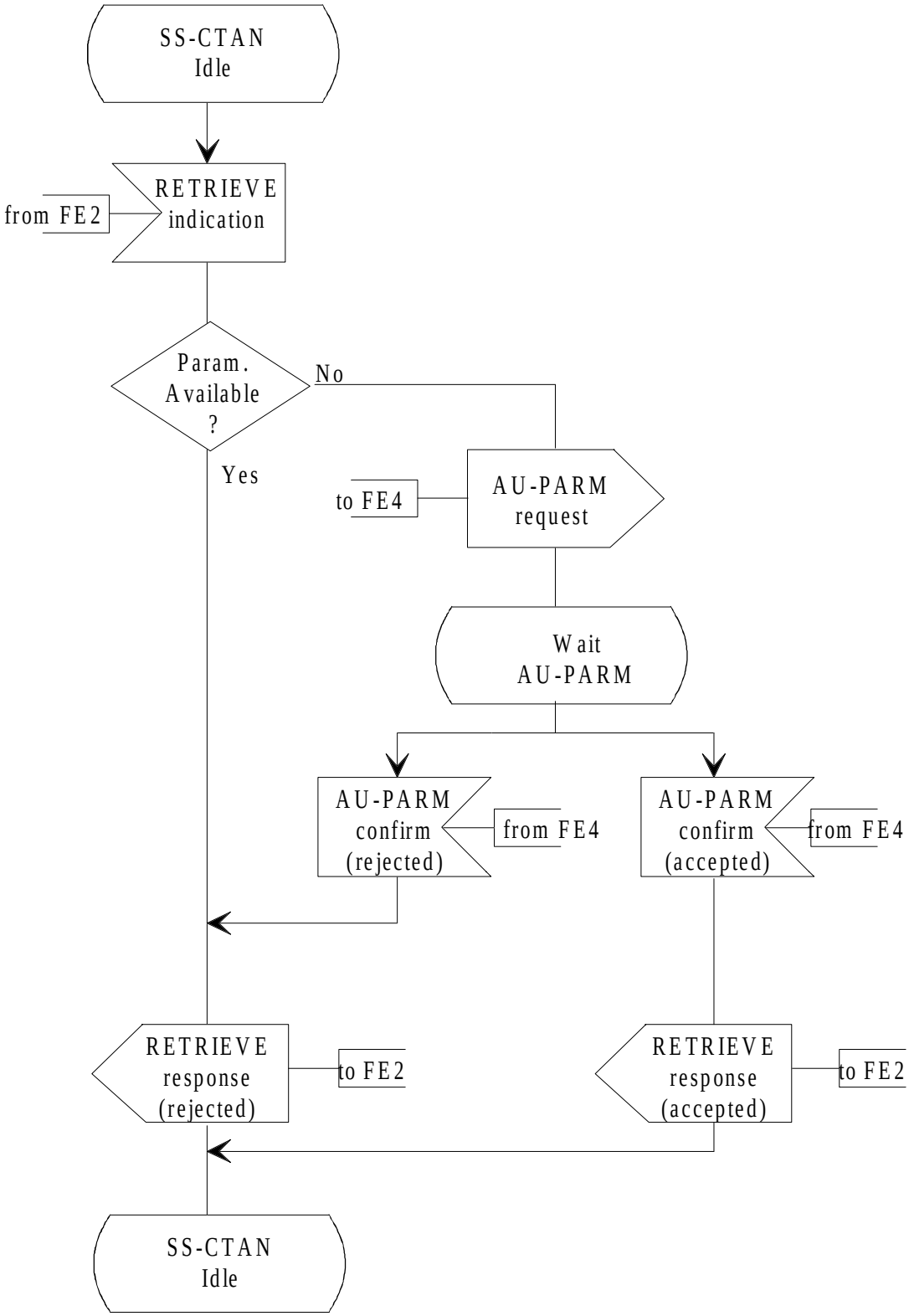


Figure 19: SDL for Functional Entity FE3 (part 1)

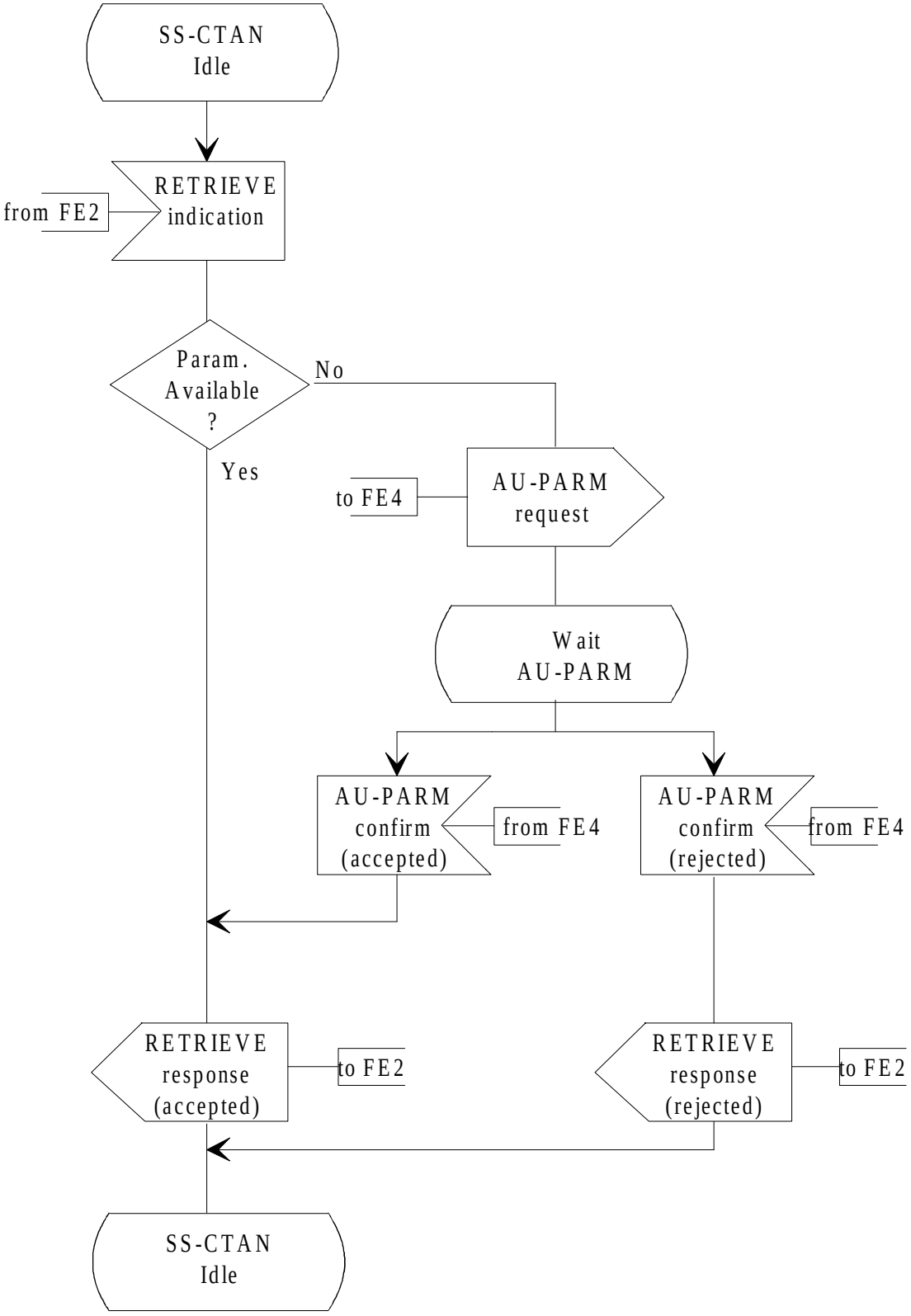


Figure 19: SDL for Functional Entity FE3 (part 2)

7.4.4 Behaviour of FE4

Figure 20 shows the SDL diagram for the functional entity FE4.

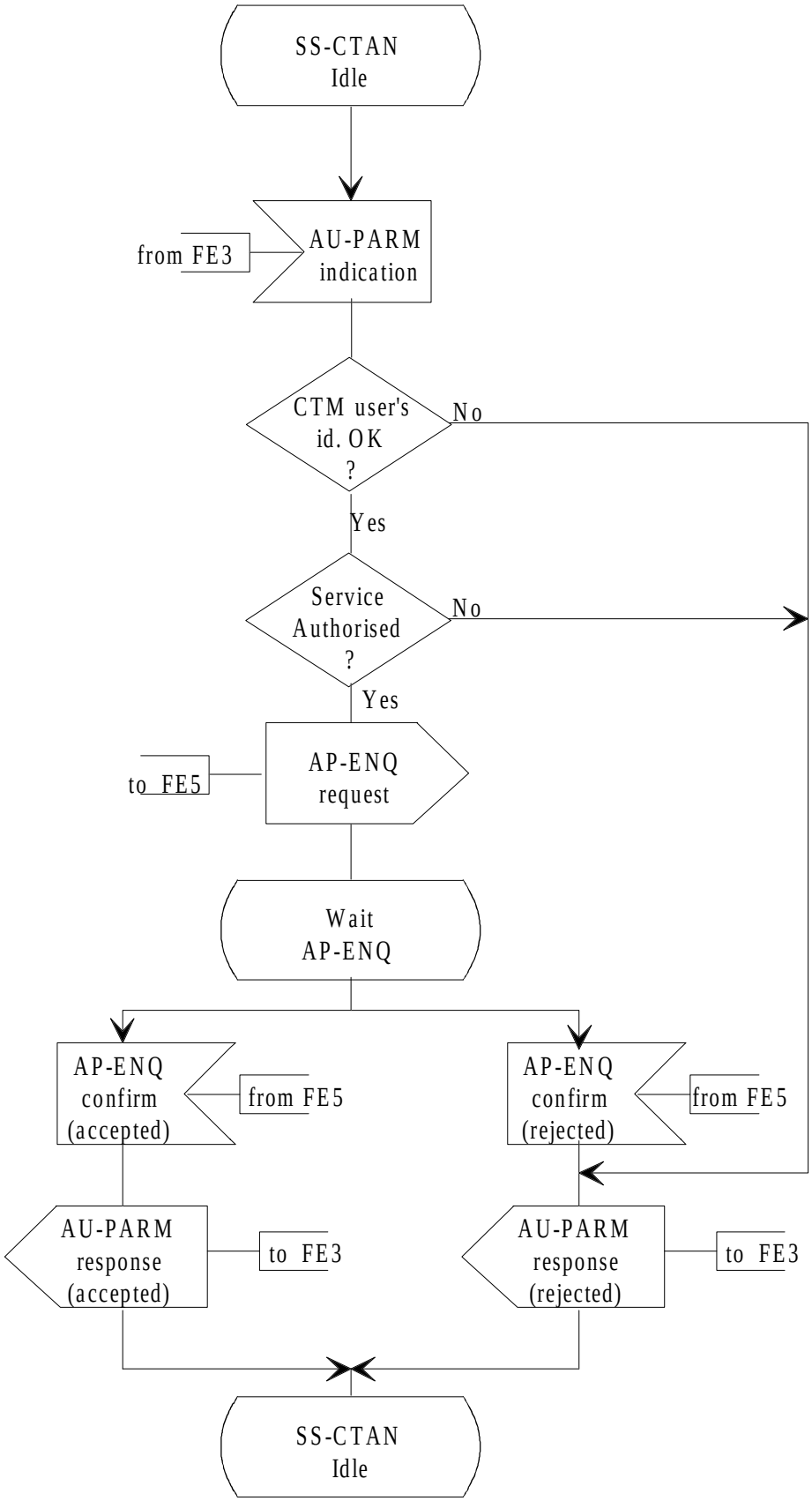


Figure 20: SDL for Functional Entity FE4

7.4.5 Behaviour of FE5

Figure 21 shows the SDL diagram for the functional entity FE5.

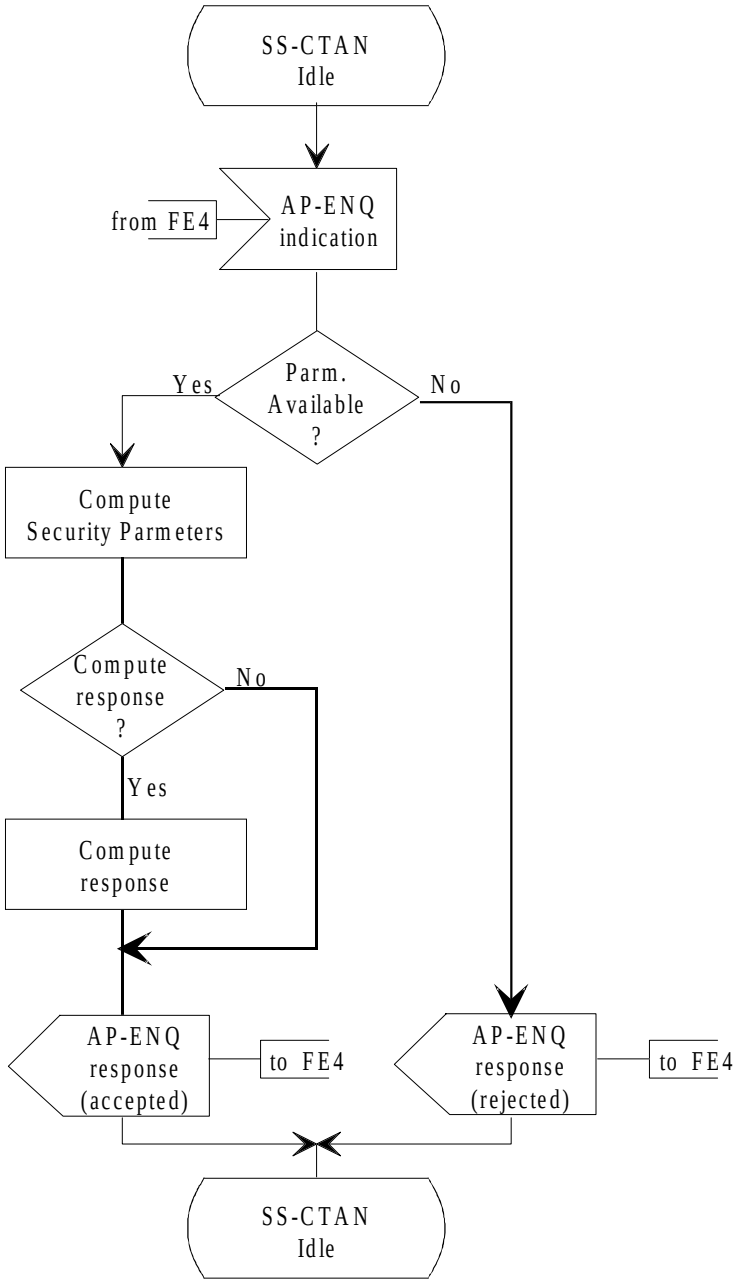


Figure 21: SDL for Functional Entity FE5

7.5 Functional Entity Actions (FEAs)

The following functional entity actions shall take place at the points indicated in the information flow sequences in subclause 7.3.1.

7.5.1 FEAs 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 CTM user.

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

7.5.2 FEAs 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.

7.5.3 FEAs 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.

7.5.4 FEAs of FE4

401 Receive AU-PARM-indication from FE3 and test if the provided CTM user's identity is valid.
If the CTM user's identity is valid then test if the CTM user is authorized for the service.
If the CTM user is authorized for the service then send AP-ENQ-request to FE5.
If the CTM user is not authorized for the service then send AU-PARM-response (rejected) to FE3.
If the CTM 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.

7.5.5 FEAs of FE5

501 Receive AP-ENQ-indication from FE4requesting 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.

7.6 Allocation of functional entities to physical locations

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

Table 11: Allocation of FEs to physical entities

	FE1	FE2	FE3	FE4	FE5
Scenario 1	FP	FP	Visitor PINX	Home PINX	Authentication Server
Scenario 2	FP	Visitor PINX	Visitor PINX	Home PINX	Authentication Server
Scenario 3	Visitor PINX	Visitor PINX	Visitor PINX	Home PINX	Authentication Server

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

7.7 Interworking Considerations

Not applicable.

History

Document history			
September 1996	Public Enquiry	PE 114:	1996-09-23 to 1997-01-17
April 1997	Vote	V 9726:	1997-04-29 to 1997-06-27