3GPP TSG_CN
Plenary Meeting #9, Oahu, Hawaii
20th – 22nd September 2000.

Tdoc NP-000498

Source: TSG_N WG 4

Title: CRs to R00 Work Item Security

Agenda item:

Document for: APPROVAL

Introduction:

This document contains 2 CRs on R00 Work Item Security, that have been agreed by TSG_N WG4, and is forwarded to TSG_N Plenary meeting #9 for approval.

SM	TDoc	SPEC	CR	REV	PHAS	VERS	SUBJECT	CAT
CN9	N4-000541	29.002	160		R00	4.0.1	AUTN and AUTS parameter length	A
CN9	N4-000744	29.002	161	2	R00	4.0.1	Clarification on Authentication Failure Report ack	A

3GPP TSG CN WG4 #3
Helsinki, Finland, 17-21 Jul 2000

Document N4-000541
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

29.002	**CR**	**160**	Current Version:	4.0.1

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	CN#09	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic	X	

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from:* ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: *(at least one should be marked with an X)* (U)SIM [ ] ME [ ] UTRAN / Radio [ ] Core Network [X]

Source: N4 **Date:** 2000-07-19

Subject: AUTS and AUTN parameter length

Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction		**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release	X		Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	
				Release 00	X

Reason for change: Mirror CR to 29.002-151

Clauses affected: 17.7.1

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other GSM core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

17.7.1 Mobile Service data types

```
MAP-MS-DataTypes {
   ccitt identified-organization (4) etsi (0) mobileDomain (0)
   gsm-Network (1) modules (3) map-MS-DataTypes (11) version6 (6)}

DEFINITIONS

IMPLICIT TAGS

::=

BEGIN

EXPORTS

      -- location registration types
      UpdateLocationArg,
      UpdateLocationRes,
      CancelLocationArg,
      CancelLocationRes,
      PurgeMS-Arg,
      PurgeMS-Res,
      SendIdentificationArg,
      SendIdentificationRes,
      UpdateGprsLocationArg,
      UpdateGprsLocationRes,
      IST-SupportIndicator,


      -- handover types
      ForwardAccessSignalling-Arg,
      PrepareHO-Arg,
      PrepareHO-Res,
      PrepareSubsequentHO-Arg,
      PrepareSubsequentHO-Res,
      ProcessAccessSignalling-Arg,
      SendEndSignal-Arg,
      SendEndSignal-Res,


      -- authentication management types
      SendAuthenticationInfoArg,
      SendAuthenticationInfoRes,
      AuthenticationFailureReportArg,
   AuthenticationFailureReportRes,

      -- security management types
      EquipmentStatus,
      Kc,

      -- subscriber management types
      InsertSubscriberDataArg,
      InsertSubscriberDataRes,
      DeleteSubscriberDataArg,
      DeleteSubscriberDataRes,
      SubscriberData,
      ODB-Data,
      SubscriberStatus,
      ZoneCodeList,
      maxNumOfZoneCodes,
      O-CSI,
   D-CSI,
      O-BcsmCamelTDPCriteriaList,
      T-BCSM-CAMEL-TDP-CriteriaList,
      SS-CSI,
      ServiceKey,
      DefaultCallHandling,
      CamelCapabilityHandling,
      BasicServiceCriteria,
      SupportedCamelPhases,
      maxNumOfCamelTDPData,
      CUG-Index,
      CUG-Interlock,
      InterCUG-Restrictions,
      IntraCUG-Options,
      NotificationToMSUser,
   IST-AlertTimerValue,
      T-CSI,
      T-BcsmTriggerDetectionPoint,
```

```
      -- fault recovery types
      ResetArg,
      RestoreDataArg,
      RestoreDataRes,

      -- subscriber information enquiry types
      ProvideSubscriberInfoArg,
      ProvideSubscriberInfoRes,
      SubscriberInfo,
      LocationInformation,
      SubscriberState,

      -- any time information enquiry types
      AnyTimeInterrogationArg,
      AnyTimeInterrogationRes,

      -- any time information handling types
      AnyTimeSubscriptionInterrogationArg,
      AnyTimeSubscriptionInterrogationRes,
      AnyTimeModificationArg,
      AnyTimeModificationRes,

      -- subscriber data modification notification types
      NoteSubscriberDataModifiedArg,
      NoteSubscriberDataModifiedRes,

      -- gprs location information retrieval types
      SendRoutingInfoForGprsArg,
      SendRoutingInfoForGprsRes,

      -- failure reporting types
      FailureReportArg,
      FailureReportRes,

      -- gprs notification types
      NoteMsPresentForGprsArg,
      NoteMsPresentForGprsRes,

      -- Mobility Management types
   NoteMM-EventArg,
      NoteMM-EventRes



;

IMPORTS
      maxNumOfSS,
      SS-SubscriptionOption,
      SS-List,
      SS-ForBS-Code,
      Password
FROM MAP-SS-DataTypes {
   ccitt identified-organization (4) etsi (0) mobileDomain (0)
   gsm-Network (1) modules (3) map-SS-DataTypes (14) version6 (6)}

      SS-Code
FROM MAP-SS-Code {
   ccitt identified-organization (4) etsi (0) mobileDomain (0)
   gsm-Network (1) modules (3) map-SS-Code (15) version6 (6)}

      Ext-BearerServiceCode
FROM MAP-BS-Code {
   ccitt identified-organization (4) etsi (0) mobileDomain (0)
   gsm-Network (1) modules (3) map-BS-Code (20) version6 (6)}

      Ext-TeleserviceCode
FROM MAP-TS-Code {
   ccitt identified-organization (4) etsi (0) mobileDomain (0)
   gsm-Network (1) modules (3) map-TS-Code (19) version6 (6)}


      AddressString,
   ISDN-AddressString,
      ISDN-SubaddressString,
      FTN-AddressString,
      AccessNetworkSignalInfo,
      IMSI,
      TMSI,
      HLR-List,
      LMSI,
```

```
      Identity,
      GlobalCellId,
      CellGlobalIdOrServiceAreaIdOrLAI,
      Ext-BasicServiceCode,
      NAEA-PreferredCI,
      EMLPP-Info,
      MC-SS-Info,
      SubscriberIdentity,
      AgeOfLocationInformation,
      LCSClientExternalID,
      LCSClientInternalID,
      Ext-SS-Status


FROM MAP-CommonDataTypes {
   ccitt identified-organization (4) etsi (0) mobileDomain (0)
   gsm-Network (1) modules (3) map-CommonDataTypes (18) version6 (6)}

      ExtensionContainer
FROM MAP-ExtensionDataTypes {
   ccitt identified-organization (4) etsi (0) mobileDomain (0)
   gsm-Network (1) modules (3) map-ExtensionDataTypes (21) version6 (6)}

      AbsentSubscriberDiagnosticSM
FROM MAP-ER-DataTypes {
   ccitt identified-organization (4) etsi (0) mobileDomain (0)
   gsm-Network (1) modules (3) map-ER-DataTypes (17) version6 (6)}


;


-- location registration types

UpdateLocationArg ::= SEQUENCE {
     imsi                                IMSI,

     msc-Number                          [1] ISDN-AddressString,
     vlr-Number                          ISDN-AddressString,
     lmsi                                [10] LMSI OPTIONAL,
     extensionContainer                  ExtensionContainer                OPTIONAL,
     ... ,
     vlr-Capability                      [6] VLR-Capability                OPTIONAL }

VLR-Capability ::= SEQUENCE{
     supportedCamelPhases                [0] SupportedCamelPhases          OPTIONAL,
     extensionContainer                  ExtensionContainer                OPTIONAL,
     ... ,
     solsaSupportIndicator               [2] NULL                          OPTIONAL,
     istSupportIndicator                 [1] IST-SupportIndicator          OPTIONAL,
     superChargerSupportedInServingNetworkEntity   [3] SuperChargerInfo    OPTIONAL,
     longFTN-Supported                   [4]  NULL                         OPTIONAL }

SuperChargerInfo ::= CHOICE {
     sendSubscriberData                  [0] NULL,
     subscriberDataStored                [1] AgeIndicator }

AgeIndicator ::= OCTET STRING (SIZE (1..6))
     -- The internal structure of this parameter is implementation specific.

IST-SupportIndicator ::=  ENUMERATED {
     basicISTSupported                   (0),
     istCommandSupported                 (1),
     ...}
-- exception handling:
-- reception of values > 1 shall be mapped to ' istCommandSupported '

UpdateLocationRes ::= SEQUENCE {
     hlr-Number                          ISDN-AddressString,

     extensionContainer                  ExtensionContainer                OPTIONAL,
     ... }
```

```
CancelLocationArg ::= [3] SEQUENCE {
     identity                         Identity,
     cancellationType                 CancellationType                 OPTIONAL,
     extensionContainer               ExtensionContainer               OPTIONAL,
     ...}
```

```
CancellationType ::= ENUMERATED {
     updateProcedure                  (0),
     subscriptionWithdraw             (1),
     ...}
     -- The HLR shall not send values other than listed above
```

```
CancelLocationRes ::= SEQUENCE {
     extensionContainer               ExtensionContainer               OPTIONAL,
     ...}
```

```
PurgeMS-Arg ::= [3] SEQUENCE {
     imsi                             IMSI,
     vlr-Number                       [0] ISDN-AddressString           OPTIONAL,
     sgsn-Number                      [1]  ISDN-AddressString          OPTIONAL,
     extensionContainer               ExtensionContainer               OPTIONAL,
     ...}
```

```
PurgeMS-Res ::= SEQUENCE {
     freezeTMSI                       [0]  NULL                        OPTIONAL,
     freezeP-TMSI                     [1]  NULL                        OPTIONAL,
     extensionContainer               ExtensionContainer               OPTIONAL,
     ...}
```

```
SendIdentificationArg ::= SEQUENCE {
     tmsi                             TMSI,
     numberOfRequestedVectors         NumberOfRequestedVectors         OPTIONAL,
     -- if segmentation is used, numberOfRequestedVectors shall be present in
     -- the first segment and shall not be present in subsequent segments. If received
     -- in a subsequent segment it shall be discarded.
     segmentationProhibited           NULL                             OPTIONAL,
     -- if segmentation is prohibited the previous VLR shall not send the result
     -- within a TC-CONTINUE message.
     extensionContainer               ExtensionContainer               OPTIONAL,
     ...}
```

```
SendIdentificationRes ::= [3] SEQUENCE {
     imsi                             IMSI                             OPTIONAL,
     -- IMSI must be present if SendIdentificationRes is not segmented.
     -- If the TC-Continue segmentation option is taken the IMSI must be
     -- present in one segmented transmission of SendIdentificationRes.
     authenticationSetList            AuthenticationSetList            OPTIONAL,
     currentSecurityContext           [2]CurrentSecurityContext        OPTIONAL,
     extensionContainer               [3] ExtensionContainer           OPTIONAL,
     ...}
```

```
-- authentication management types
```

```
AuthenticationSetList ::= CHOICE {
     tripletList                      [0] TripletList,
     quintupletList                   [1] QuintupletList }
```

```
TripletList ::= SEQUENCE SIZE (1..5) OF
                                      AuthenticationTriplet
```

```
QuintupletList ::= SEQUENCE SIZE (1..5) OF
                                      AuthenticationQuintuplet
```

```
AuthenticationTriplet ::= SEQUENCE {
     rand                             RAND,
     sres                             SRES,
     kc                               Kc,
     ...}
```

```
AuthenticationQuintuplet ::= SEQUENCE {
     rand                             RAND,
     xres                             XRES,
     ck                               CK,
     ik                               IK,
     autn                             AUTN,
     ...}
```

```
CurrentSecurityContext ::= CHOICE {
     gsm-SecurityContextData              [0] GSM-SecurityContextData,
     umts-SecurityContextData             [1] UMTS-SecurityContextData }
```

```
GSM-SecurityContextData ::= SEQUENCE {
     kc                                   Kc,
     cksn                                 Cksn,
     ... }
```

```
UMTS-SecurityContextData ::= SEQUENCE {
     ck                                   CK,
     ik                                   IK,
     ksi                                  KSI,
     ... }
```

```
RAND ::= OCTET STRING (SIZE (16))
```

```
SRES ::= OCTET STRING (SIZE (4))
```

```
Kc ::= OCTET STRING (SIZE (8))
```

```
XRES ::= OCTET STRING (SIZE (4..16))
```

```
CK ::= OCTET STRING (SIZE (16))
```

```
IK ::= OCTET STRING (SIZE (16))
```

```
AUTN ::= OCTET STRING (SIZE (164..18))
```

```
AUTS ::= OCTET STRING (SIZE (142..16))
```

3GPP TSG CN WG4 #4
Seattle (WA), USA, Aug 28 - Sep 1, 2000

Document N4-000744
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

29.002	CR	161r2	Current Version:	4.0.1

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to: CN#09	For approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑	for information		non-strategic	X	

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from:* ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: *(at least one should be marked with an X)* (U)SIM [ ] ME [ ] UTRAN / Radio [ ] Core Network [X]

Source: N4 **Date:** 2000-08-31

Subject: Clarification on Authentication Failure Report ack

Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction		**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release	X		Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	
				Release 00	X

Reason for change: Mirror CR of 29.002-154r3

Clauses affected: 8.5.3.3, 25.5.7.4

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other GSM core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

8.5.3.3 Parameter use

Invoke id

See subclause 7.6.1 for the use of this parameter.

IMSI

See subclause 7.6.2 for the use of this parameter.

Failure Cause

See subclause 7.6.7 for use of this parameter.

User error

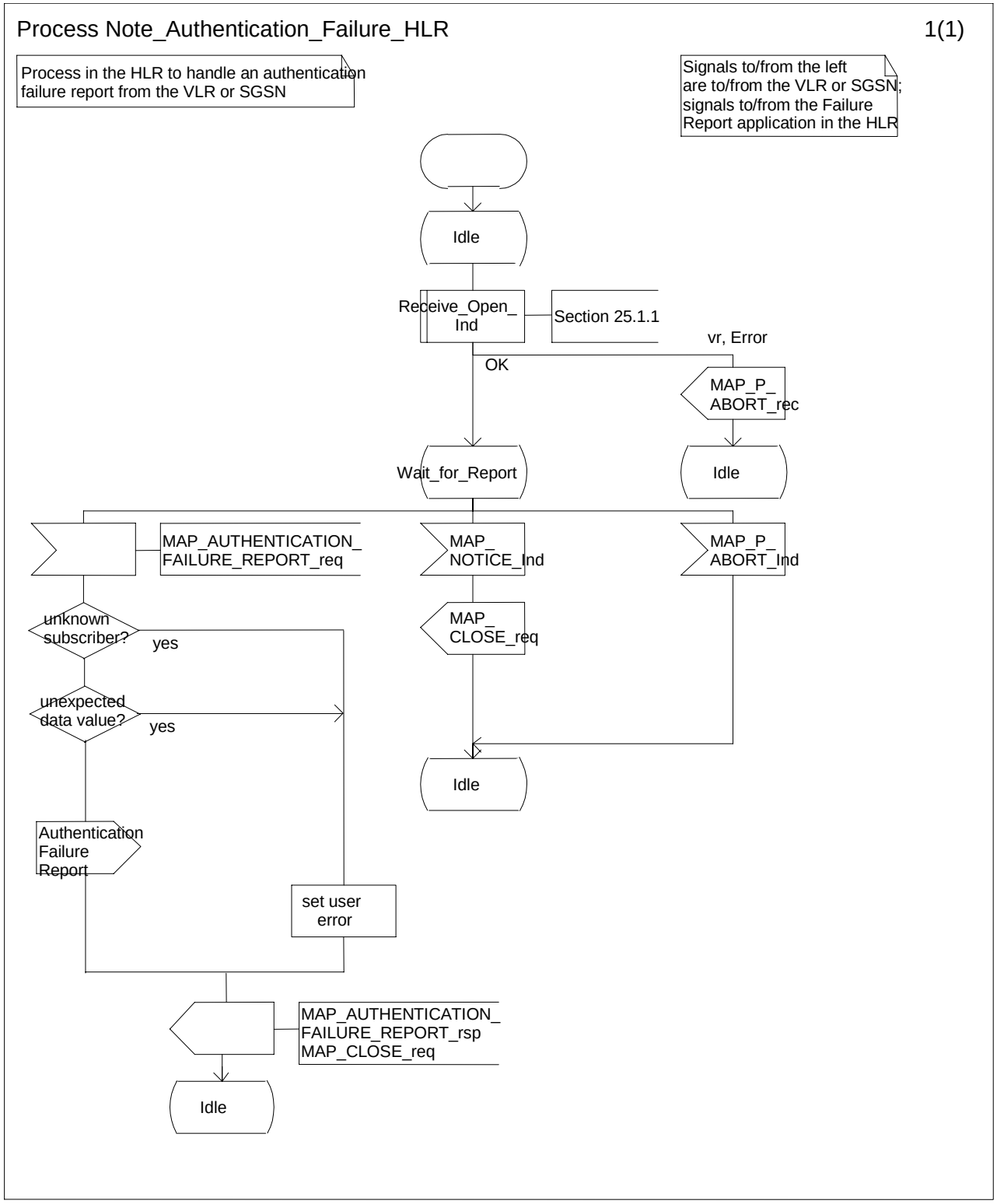
This parameter is sent by the responder upon unsuccessful outcome of the service, and then takes one of the following values defined in subclause 7.6.1:

- Unknown Subscriber;
- System Failure;
- Unexpected Data Value.~~;~~
- ~~Data Missing.~~

Provider error

These are defined in subclause 7.6.

25.5.7.4 Process in the HLR


Process Note_Authentication_Failure_HLR
1(1)
Process in the HLR to handle an authentication failure report from the VLR or SGSN
Signals to/from the left are to/from the VLR or SGSN; signals to/from the Failure Report application in the HLR
Idle
Receive_Open_Ind
Section 25.1.1
vr, Error
OK
MAP_P_ABORT_rec
Wait_for_Report
Idle
MAP_AUTHENTICATION_FAILURE_REPORT_req
MAP_NOTICE_Ind
MAP_P_ABORT_Ind
unknown subscriber?
yes
MAP_CLOSE_req
unexpected data value?
yes
Idle
Authentication Failure Report
set user error
MAP_AUTHENTICATION_FAILURE_REPORT_rsp
MAP_CLOSE_req
Idle

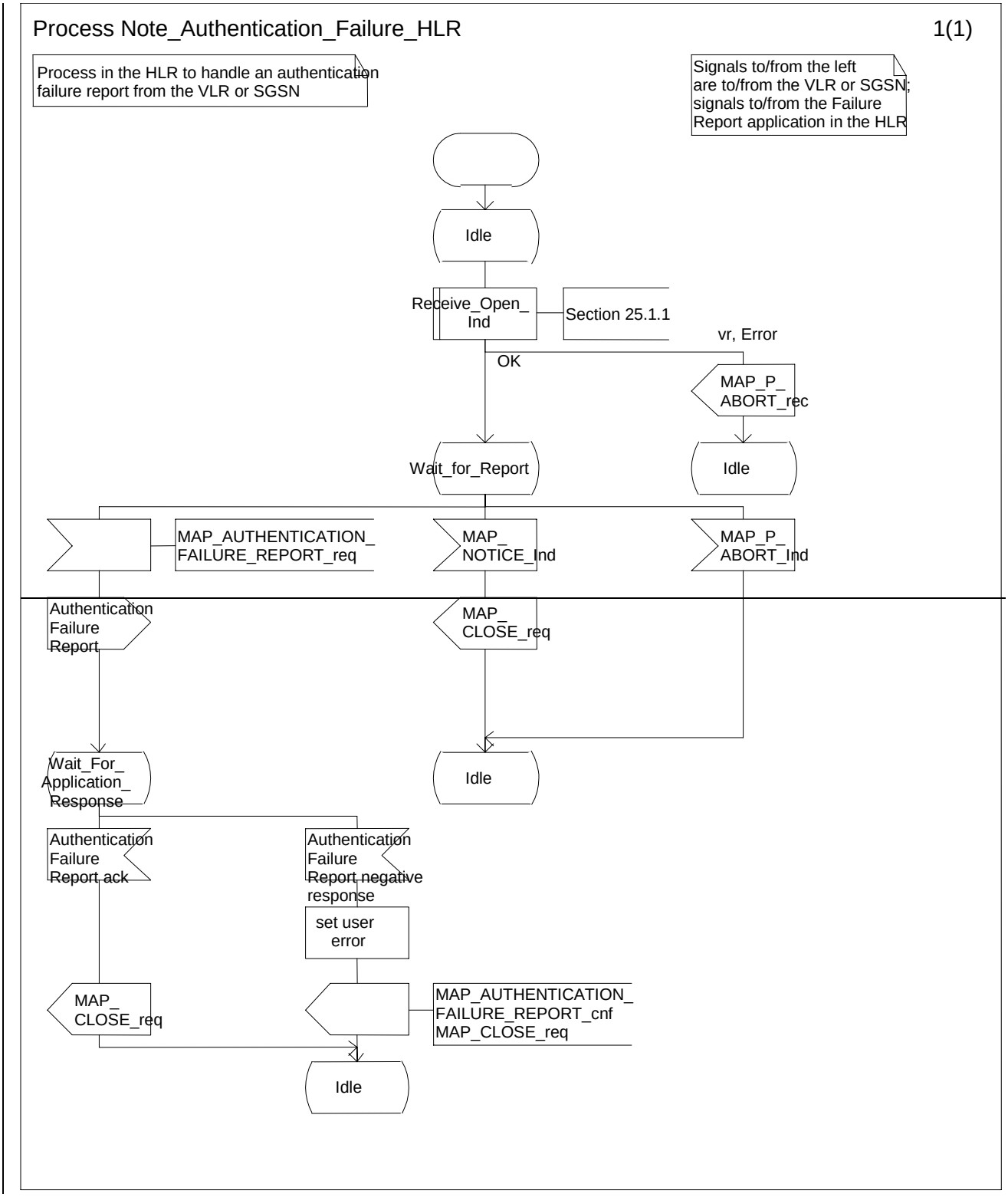


Figure 25.6/10: Process Note_Authentication_Failure_HLR