EUROPEAN TELECOMMUNICATION STANDARD

FINAL DRAFT
pr ETS 300 788

April 1997

Source: ETSI EP DECT

Reference: DE/DECT-010064

ICS: 33.020

Key words: CTM, DECT, GSM, ISDN, mobility, radio, stage 2

Digital Enhanced Cordless Telecommunications (DECT); Global System for Mobile communications (GSM); Integrated Services Digital Network (ISDN); DECT access to GSM via ISDN; 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 European Telecommunication Standard (ETS) has been produced by the Digital Enhanced Cordless Telecommunications (DECT) Project of the European Telecommunications Standards Institute (ETSI), and is now submitted for the Voting phase of the ETSI standards approval procedure.

Proposed transposition dates	
Date of latest announcement of this ETS (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

Blank page

1 Scope

This European Telecommunication Standard (ETS) defines the functional capabilities and information flows for the scenarios where Global System for Mobile communications (GSM) basic services are provided via the Digital Enhanced Cordless Telecommunications System (DECT) air interface for the case that the DECT network elements are interconnected with the GSM Public Land Mobile Network (PLMN) via Integrated Services Digital Network (ISDN) interfaces.

The general description of the service requirements are specified in ETS 300 787 [1].

The following core features are covered by this ETS:

- outgoing calls;
- emergency calls;
- incoming calls;
- location updating, location cancellation;
- IMSI attach/detach;
- TMSI reallocation procedure (temporary identity assign);
- IMSI authentication;
- ciphering;
- identity request.

Handover, which is another Mobility Management (MM) service, is outside the scope of this ETS.

The service is produced in three stages according to the method specified in CCITT Recommendation I.130 [6]. Stage 2 identifies the Functional Entities (FEs) involved in the service and the information flows between them. This ETS is specified according to the methodology specified in CCITT Recommendation Q.65 [7].

The purpose of the stage 2 specification is to guide and constrain the work on signalling protocols at stage 3, while fulfilling the requirements of stage 1. Stage 1 and stage 3 are defined in separate standards.

This ETS distinguishes DECT access networks from the global network. The DECT access network provides the point of attachment for the served user and ensures a transparent access to the GSM services. The global network is the GSM PLMN or network of GSM PLMNs which provides the served user with the global service specified in this ETS. The specification of information flows within the global network (e.g. between Mobile Switching Centres (MSCs), Home Location Register (HLR) and Visitor Location Register (VLR)) is beyond the scope of this ETS.

Furthermore, conformance to this ETS is met by conforming to the stage 3 standards which fulfil the requirements of this ETS that are relevant to the equipment for which the stage 3 standard applies. Therefore no method of testing is provided for this ETS.

2 Normative references

This 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 to this ETS only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] ETS 300 787: "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications / Global System for Mobile communications (DECT/GSM); DECT access to GSM via Integrated Services Digital Network (ISDN); General description of service requirements".

[2] ETS 300 444: "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT); Generic Access Profile (GAP)".

[3] ETS 300 370: "Radio Equipment and Systems (RES); Digital European Cordless Telecommunications/Global System for Mobile communications (DECT/GSM) inter-working profile; Access and mapping (Protocol/procedure description for 3,1 kHz speech service)".

[4] ETS 300 557: "Digital cellular telecommunications system (Phase 2); Mobile radio interface layer 3 specification (GSM 04.08)".

[5] ITU-T Recommendation Q.71 (1993): "ISDN circuit mode switched bearer services".

[6] CCITT Recommendation I.130 (1988): "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".

[7] CCITT Recommendation Q.65 (1988): "Stage 2 of the method for the characterization of services supported by an ISDN".

[8] ETS 300 434-1: "Radio Equipment and Systems (RES); Digital Enhanced Cordless Telecommunications (DECT) and Integrated Services Digital Network (ISDN) interworking for end system configuration; Part 1: Interworking specification".

[9] ITU-T Recommendation Z.100: "CCITT Specification and description language (SDL)".

3 Definitions and abbreviations

3.1 Definitions

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

DECT access network: Physical entity that contains all of the elements of a DECT Fixed Part (FP) and that is attached to a GSM MSC.

NOTE 1: A DECT access network provides a transparent access to the services of the GSM PLMN. This does however not exclude that it may in addition provide services and switching capabilities to its own users.

DECT Fixed Part (FP): A physical grouping that contains all of the elements in the DECT network between the local network and the DECT air interface.

NOTE 2: A DECT FP contains the logical elements of at least one fixed radio termination, plus additional implementation specific elements.

DECT location area: The domain in which a DECT Portable Part (PP) may receive and/or make calls as a result of a single location registration in the DECT access network.

global network: The GSM PLMN or network of GSM PLMNs which provides the served user with the global service specified in this ETS.

GSM location area: The domain in which a DECT PP may receive and/or make calls as a result of a single location updating in the GSM network.

NOTE 3: A GSM location area may cover more than one DECT location area.

GSM service provider: An administration which offers global mobile telecommunication services to its subscribers.

GSM services: Services which are offered to the subscriber/user by a GSM Service Provider and which are defined by the appropriate GSM specifications.

location area: The domain in which a DECT PP may receive and/or make calls as a result of a single location registration/updating in the network.

location registration: The process whereby the position of a PP is determined to the level of one location area, and this position is updated in the network.

location updating: The process whereby the position of a PP is determined to the level of one location area, and this position is updated in the network.

NOTE 4: DECT and GSM respectively use the terms location registration and location updating for corresponding processes.

MSC area: The MSC area is the part of the network covered by an MSC. An MSC area may consist of one or several GSM location areas. An MSC area may also consist of one or several BSC areas and/or one or several DECT location areas.

network: The totality of GSM and DECT access network elements through which the GSM service provider provides its services to the served user.

Public Land Mobile Network (PLMN): A PLMN is established and operated by an administration or for the specific purpose of providing land mobile telecommunication services to the public. A PLMN may be regarded as an extension of a network (e.g. ISDN); it is a collection of MSC areas within a common numbering plan (e.g. same national destination code) and a common routeing plan. The MSCs are the functional interfaces between the fixed networks and a PLMN for call set-up. Functionally the PLMNs may be regarded as independent telecommunication entities even though different PLMNs may be interconnected through the ISDN/PISN and PDNs for forwarding of calls or network information. A similar type of interconnection may exist for the interaction between the MSCs of one PLMN.

served user: The user of a DECT PP who has a subscription with the GSM service provider. The DECT PP accepts the GSM Subscriber Identity Module (SIM) and optionally the DECT DAM with a GSM Application.

NOTE 5: For the purpose of this ETS no distinction is made between the served user and its associated DECT PP.

3.2 Abbreviations

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

CC	Call Control (functional entity)
CCA	Call Control Agent (functional entity)
DECT	Digital Enhanced Cordless Telecommunications
FE	Functional Entity
FP	Fixed Part
GSM	Global System for Mobile communications
HLR	Home Location Register
IMEI	International Mobile Equipment Identity
IMEISV	IMEI Software Version number
IMSI	International Mobile Subscriber Identity (GSM)
IPEI	International Portable Equipment Identity
IPUI	International Portable User Identity (DECT)
ISDN	Integrated Services Digital Network
MM	Mobility Management
MSC	Mobile Switching Centre
PABX	Private Automatic Branch Exchange
PDN	Packet Data Network
PISN	Private Integrated Services Network
PLMN	Public Land Mobile Network
PP	Portable Part
RAND	Random number
RES	A Response calculated by a PP
SDL	Specification and Description Language
SIM	Subscriber Identity Module
SRES	A GSM specific authentication RES calculated by the GSM SIM or the DAM
TE	Terminal Equipment
TMSI	Temporary Mobile Subscriber Identity (GSM)
TPUI	Temporary Portable User Identity
VLR	Visitor Location Register

4 Mobility management features

4.1 Functional model

4.1.1 Functional model description

The functional model for the MM features shall be as shown in figure 1.

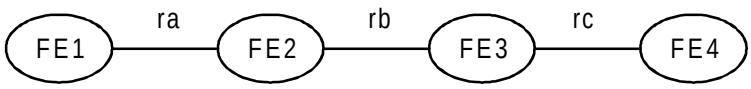


Figure 1: Functional model for MM features

The FEs for the MM features shall be as follows:

FE1: Mobile user's MM agent;
FE2: Currently visited DECT access network MM control;
FE3: Global network MM control;
FE4: Previously visited DECT access network MM control.

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.

4.1.2 Description of functional entities

4.1.2.1 Mobile user's MM agent, FE1

This FE performs the user specific part of the MM features. It initiates and/or performs MM procedures on behalf of the mobile user. FE1 is also responsible for passing information to the mobile user, if applicable.

4.1.2.2 Currently visited DECT access network MM control, FE2

FE2 performs the DECT access network specific part of the MM features at the current location of the served user. If involvement of the global network is required, FE2 cooperates with FE3 in providing the required feature.

FE2 receives information from FE1 when a MM procedure has been invoked. FE2 also can trigger FE1 to perform actions for MM procedures initiated by the network (either by FE2 itself or on initiative of FE3).

NOTE: The possible information transfer within sub-entities in FE2 (e.g. when FE2 consists of more than one DECT location area) is out of the scope of this ETS.

4.1.2.3 Global network MM control, FE3

FE3 performs the global network specific part of the MM features, i.e. the mobility actions which are of global significance.

FE3 receives information from FE2 that a MM procedure has been invoked. FE3 also can trigger FE1/FE2 to perform actions for network initiated MM procedures.

NOTE: The possible information transfer within sub-entities in FE3 (e.g. between MSC's, HLR and VLR) is out of the scope of this ETS.

4.1.2.4 Previously visited DECT access network MM control, FE4

FE4 performs the DECT access network specific part of the MM features at the previous location of the served user. FE4 receives information from FE3 that a served user is no longer in the domain controlled by FE4. On receipt of such information, FE4 will delete all temporary data stored for that user.

NOTE: The possible information transfer within sub-entities in FE4 (e.g. when FE4 consists of more than one DECT location area) is out of the scope of this ETS.

4.1.3 Relationship of functional model to basic call functional model

The functional model for MM features is independent of the functional model for basic call.

4.2 Information flows

4.2.1 Definition of information flows

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

4.2.1.1 ra-detach

ra-detach is an unconfirmed information flow across ra from FE1 to FE2 to achieve a deactivation of the user's terminal in the network.

Table 1: Contents of ra-detach

Service element	Request	Notes
Portable identity	M	- Contains the user's DECT identity - If "temporary identity" is not available, the only allowed value of "portable identity" shall be of type IPUI, with IPUI-type R, i.e. the IPUI shall incorporate an IMSI - Other allowed values (of type TPUI, IPEI) may be used in the non-DECT/GSM interworking case or when "mobile identity" is also included.
Temporary identity	O	- Contains the user's GSM temporary identity - Allowed value is of type GSM TMSI - Shall be included if previously received from the network before
IPEI: International Portable Equipment Identity IPUI: International Portable User Identity TPUI: Temporary Portable User Identity TMSI: Temporary Mobile Subscriber Identity		

4.2.1.2 ra-identity-request

ra-identity-request is a confirmed information flow across ra between FE2 and FE1 which is used by FE2 to obtain one of the user's terminal identities.

Table 2: Contents of ra-identity-request

Service element	Request	Confirm	Notes
Identity type	M	-	- This service element indicates the type of identity requested by the network. - For the scope of this ETS the only values of relevance are the types "Temporary identity (TMSI)", "user's portable identity (IPUI)" and "portable equipment identity (IPEI)".
Portable identity	-	O	- Contains either the user's or the equipment's DECT identity (i.e. IPUI or IPEI) - If the requested Identity type is "User's portable identity", then this service element shall include a value of type IPUI with IPUI-type R, i.e. shall include an IMSI. - If the requested Identity type is "Portable equipment identity", this service element shall include an IPEI-value
Temporary identity	-	O	- Contains the user's temporary GSM identity, the TMSI - Shall be included if the requested Identity type is "Temporary identity", and if this identity is available.

4.2.1.3 ra-location-registration

ra-location-registration is a confirmed information flow across ra between FE1 and FE2 which is used to inform FE2 that the served user has roamed to another DECT location area or that a non-roaming served user is now able to receive incoming calls.

Table 3: Contents of ra-location-registration

Service element	Request	Confirm	Notes
Portable identity	M	-	- Contains the user's DECT identity - Allowed value is of type IPUI, TPUI. The IPUI-type shall be R, i.e. the IPUI shall incorporate an IMSI
Fixed identity	O	-	DECT specific identity which is not of relevance for DECT/GSM interworking case, and therefore out of the scope of this ETS
Location area identity	O	M	- Can contain the DECT location area identity and the GSM location area identity - In the "request/indication" this element may include the previous DECT location area. If available, also the GSM location area identity shall be included. - In the "resp/conf" this element shall include the current DECT location area identity, and, if applicable and available, also the GSM location area identity.
Use TPUI	-	O	To mandate the use of the temporary identity
Temporary identity	O	O	- Contains the user's GSM temporary identity, the GSM TMSI. - This identity shall be included in the "request/indication" if previously received from the network. - It shall be included in the "resp/conf" if a new identity has been provided by the global network.
Cipher key sequence number	M	-	This parameter gives information to FE2 on the ciphering key that is intended to be used by FE1
Terminal / setup capabilities and model identifier	O	-	May be needed to generate an IMEISV later on
Result	-	M	This takes the values "accepted" and "rejected"
Cause of rejection	-	O	- Only present if result is "rejected". - At least the following values are allowed: "user identity not known", "served user not permitted to register in the current location area", "served user failed authentication", "location registration temporarily not possible".
Duration	-	O	If present this element defines for how long at least the location registration and temporary identity (if provided) are valid

4.2.1.4 ra-temporary-identity-assign

ra-temporary-identity-assign is a confirmed information flow across ra between FE2 and FE1 which is used to assign or delete a temporary identity to/from the user's terminal.

Table 4: Contents of ra-temporary-identity-assign

Service Element	Request	Confirm	Notes
Portable identity	O	-	This service element is not relevant for the DECT/GSM interworking case
GSM location area identity	M	-	Contains the GSM location area for which the newly assigned temporary identity is valid
Temporary identity	M	-	Contains the user's temporary GSM identity (TMSI). For the DECT/GSM interworking case, this element is mandatory
Result	-	M	Accepted or rejected
Cause of rejection	-	O	May be included if the result is "rejected"

4.2.1.5 ra-temporary-identity-result

ra-temporary-identity-result is an unconfirmed information flow across ra from FE1 to FE2 which is used to confirm the allocation of a (new) temporary identity to the user's terminal as a result of a successful location registration procedure.

Table 5: Contents of ra-temporary-identity-result

Service Element	Request	Notes
Result	M	Accepted or rejected
Cause of rejection	O	May be included if the result is "rejected"

4.2.1.6 ra-authenticate

ra-authenticate is a confirmed information flow across ra between FE2 and FE1 which is used to authenticate the mobile user.

Table 6: Contents of ra-authenticate

Service Element	Request	Confirm	Notes
Authentication type	M	-	Indicates "GSM authentication"
Random number (RAND)	M	-	Contains a random number, which is used for the calculation of the authentication result (RAND)
Cipher key sequence number	M	-	This number must be used by the terminal for association with the calculated cipher key, which results from the auth/ciphering key generation algorithm
Result	-	M	Indicates whether the request for authentication is accepted or rejected
Authentication result		O	Included if the result is "accepted", contains the calculated result of the authentication (RES)
Cause of rejection	-	O	May be included if Result is "rejected", and indicates the reason why the authentication request could not be accepted

4.2.1.7 ra-ciphering-setting

ra-ciphering-setting is a confirmed information flow across ra between FE2 and FE1 which is used to establish ciphering for the radio link.

Table 7: Contents of ra-ciphering-setting

Service Element	Request	Confirm	Notes
Cipher key sequence number	M	-	Contains the number of the cipher key which shall be used to encrypt the radio link The cipher key number has been received previously in one of the following procedures: DECT location registration, paging, PP initiated call establishment or the value has been given from the MSC during a previous authentication procedure. The latest received value is used.
Result	-	M	Accepted or rejected
Cause of rejection	-	O	May be included if the result is "rejected"

4.2.1.8 rb-detach

rb-detach is an unconfirmed information flow across rb from FE2 to FE3 to achieve a deactivation of the user's terminal in the global network.

Table 8: Contents of rb-detach

Service Element	Request	*Notes*
Terminal capabilities	M	Shall indicate a revision level of Phase 2 or higher and the support of encryption A 5/1
Mobile identity	M	- Contains the user's GSM identity - Allowed values: GSM TMSI or IMSI - If TMSI is available, then this shall be used instead of IMSI.

4.2.1.9 rb-identity-request

rb-identity-request is a confirmed information flow across rb between FE3 and FE2 which is used by FE3 to obtain one of the user's terminal identities.

Table 9: Contents of rb-identity-request

Service Element	Request	Confirm	Notes
Mobile identity	O	-	Identification of the user from which an additional identity is requested
Mobile identity type	M	-	This takes one of the values IMSI, TMSI, IMEI, IMEISV
Mobile identity	-	M	Contains the user's GSM identity of the type as requested
IMEI: International Mobile Equipment Identity IMEISV: IMEI Software Version number IMSI: International Mobile Subscriber Identity TMSI: Temporary Mobile Subscriber Identity			

4.2.1.10 rb-location-update

rb-location-update is a confirmed information flow across rb between FE2 and FE3 which is used to inform FE3 that the served user has roamed to another GSM location area or that a non-roaming served user is now ready to receive incoming calls.

Table 10: Contents of rb-location-update

Service Element	Request	Confirm	Notes
Location update type	M	-	This takes the values "normal updating", "periodic updating" and "IMSI attach"
Cipher key sequence number	M	-	This parameter gives information to FE3 on the ciphering key that is intended to be used by FE1
GSM location area identity	M	M	In the "req/ind" this service element identifies the previously visited GSM location area. In the "resp/conf" the identity of the current GSM location area is given to FE2.
Terminal capabilities	M	-	Shall indicate a revision level of Phase 2 or higher and the support of encryption A 5/1.
Mobile identity	M	O	- Contains the user's GSM identity - In the "req/ind" TMSI shall be used if available. If TMSI is not available, the IMSI shall be used. - In the "resp/conf" this may contain a TMSI
Result	-	M	This takes the values "accepted" and "rejected".
Cause of rejection	-	M	At least the following values are allowed: "IMSI unknown", "illegal MS", "illegal ME", "PLMN not allowed", "location area not allowed", "national roaming not allowed in this location area". Other values are considered as abnormal values.

4.2.1.11 rb-temporary-identity-assign

rb-temporary-identity-assign is a confirmed information flow across rb between FE3 and FE2 which is used to assign or delete a temporary identity to/from the user's terminal.

Table 11: Contents of rb-temporary-identity-assign

Service Element	Request	Confirm	Notes
GSM location area identity	M	-	Contains the GSM location area for which the newly assigned mobile identity is valid
Mobile identity	M	-	Contains the user's GSM identity. The usual value is TMSI. The IMSI can be included instead, as a request to delete the current TMSI without assigning a new one.

4.2.1.12 rb-temporary-identity-accept

rb-temporary-identity-accept is an unconfirmed information flow across rb from FE2 to FE3 which is used to confirm the allocation of a (new) temporary identity to the user's terminal as a result of a successful location registration procedure. This information flow contains no service elements.

4.2.1.13 rb-authenticate

rb-authenticate is a confirmed information flow across rb between FE3 and FE2 which is used to request authentication of the mobile user.

Table 12: Contents of rb-authenticate

Service Element	Request	Confirm	Notes
Cipher key sequence number	M	-	Contains the number that is given to the cipher key which is generated during this authentication procedure
Random number	M	-	Contains a RAND, which is used for the calculation of the authentication result
Authentication result	-	M	Contains the calculated result (SRES) of the authentication

4.2.1.14 rb-authenticate-reject

rb-authenticate-reject is a unconfirmed information flow across rb between FE3 and FE2 which is used to inform FE2 that authentication has failed. This information flow contains no service elements.

4.2.1.15 rb-ciphering-setting

rb-ciphering-setting is a confirmed information flow across rb between FE3 and FE2 which is used to request ciphering for the radio link.

Table 13: Contents of rb-ciphering-setting

Service Element	Request	Confirm	Notes
Cipher key	M	-	Contains the cipher key which shall be used to encrypt the radio link

4.2.1.16 rc-location-delete

rc-location-delete is an unconfirmed information flow across rc from FE3 to FE4 which is used to inform FE4 that a user has roamed outside FE4's domain.

Table 14: Contents of rc-location-delete

Service Element	Request	Notes
Mobile identity	M	Contains the user's GSM identity

4.2.2 Relationship of information flows to basic call information flows

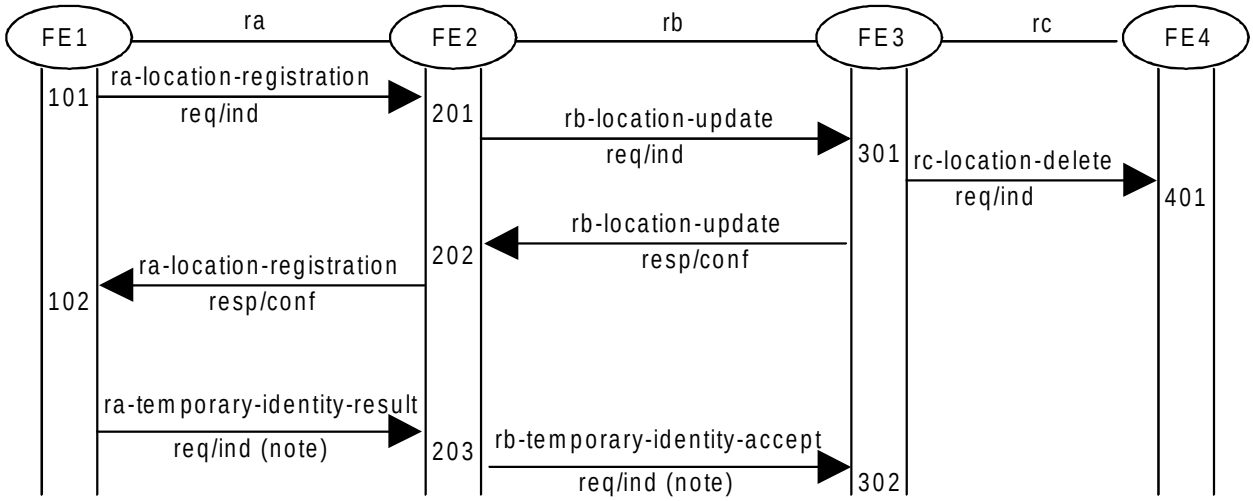
All information flows for MM are independent of basic call information flows.

4.2.3 Examples of information flow sequences

Below are examples of typical sequences of information flows. These sequences shall be taken into account at Stage 3. However, these examples are not necessarily exhaustive, and in particular may not cover all error situations, interactions with other supplementary services, etc.

4.2.3.1 Normal operation of MM features

Figure 2 shows the information flow sequence for normal operation of location registration.



NOTE: ra/rb-temporary-identity-result/accept req/ind is only sent if the network had proposed a (new) temporary identity in ra-location-registration resp/conf.

Figure 2: Normal operation of location registration

Figure 3 shows the information flow sequence for normal operation of temporary identity assignment when it is not part of the location registration procedure.

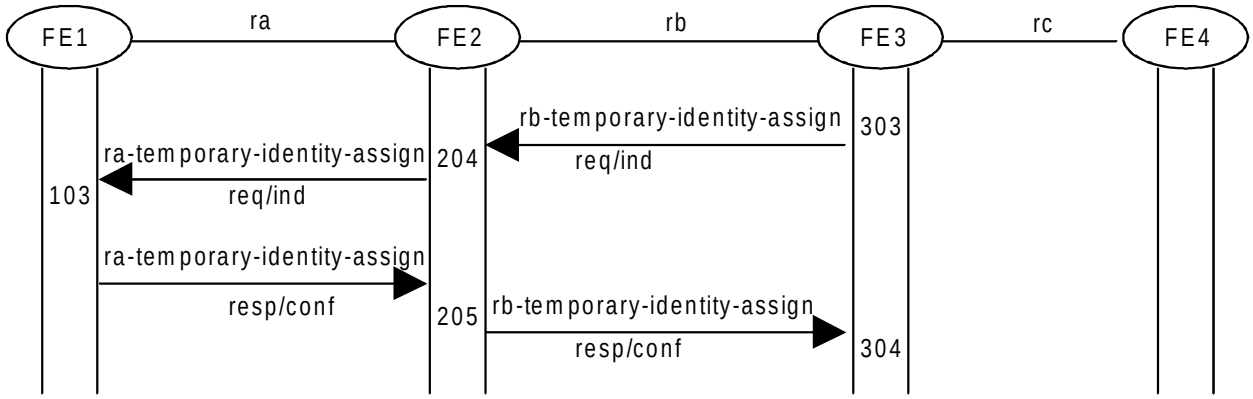
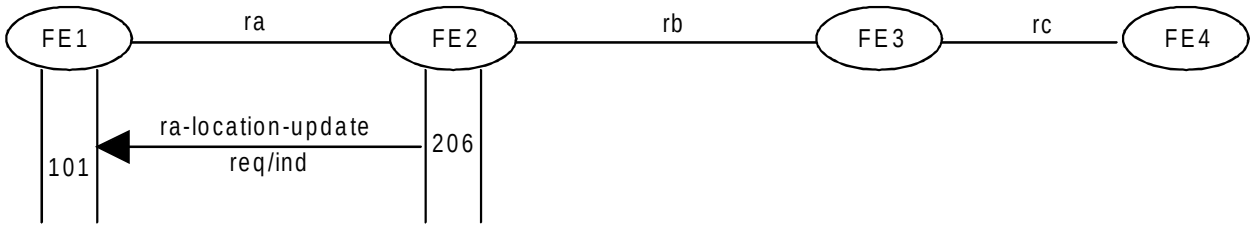


Figure 3: Normal operation of temporary identity assignment

Figure 4 shows the information flow sequence for normal operation of location registration on invitation by the network.



(Continue as for figure 2)

Figure 4: Location registration on invitation by the network

Figure 5 shows the information flow sequence for normal operation of detach.

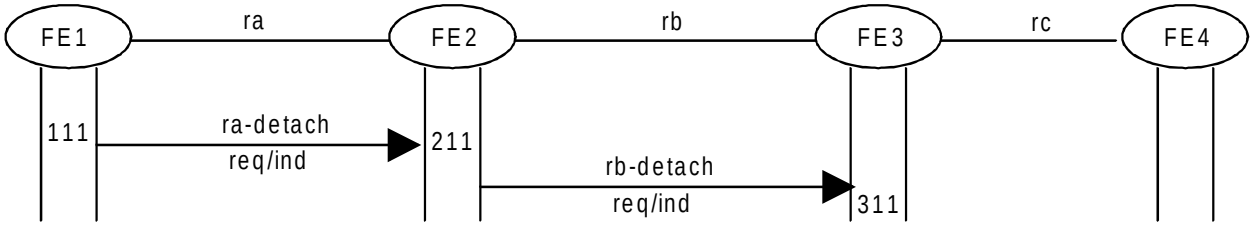


Figure 5: Normal operation of detach

Figure 6 shows the information flow sequence for normal operation of identity request.

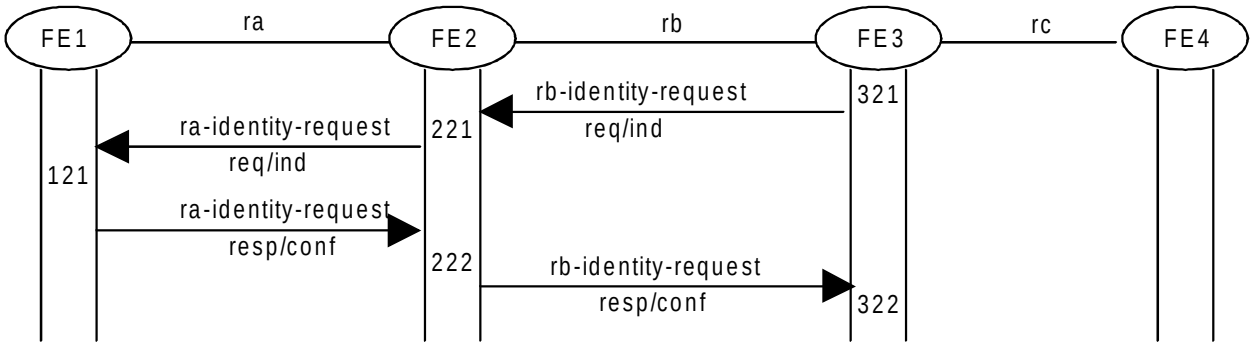


Figure 6: Normal operation of identity request

Figure 7 shows the information flow sequence for normal operation of authentication.

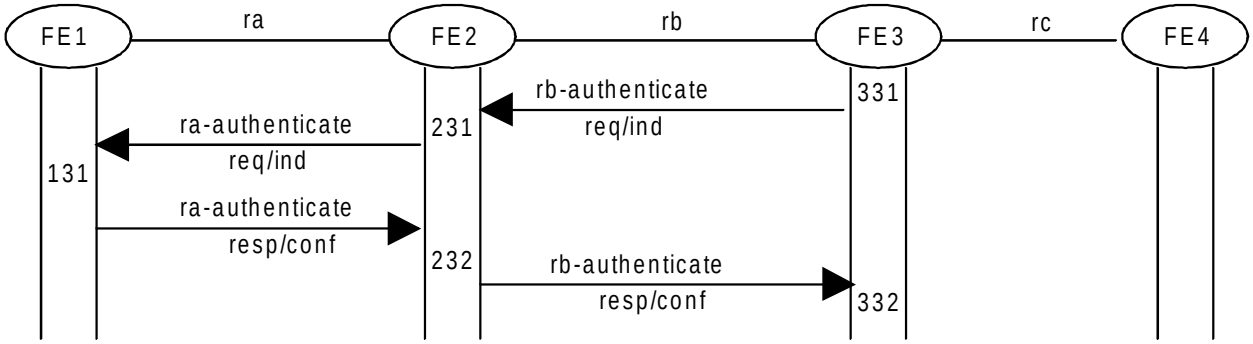


Figure 7: Normal operation of authentication

Figure 8 shows the information flow sequence for normal operation of ciphering.

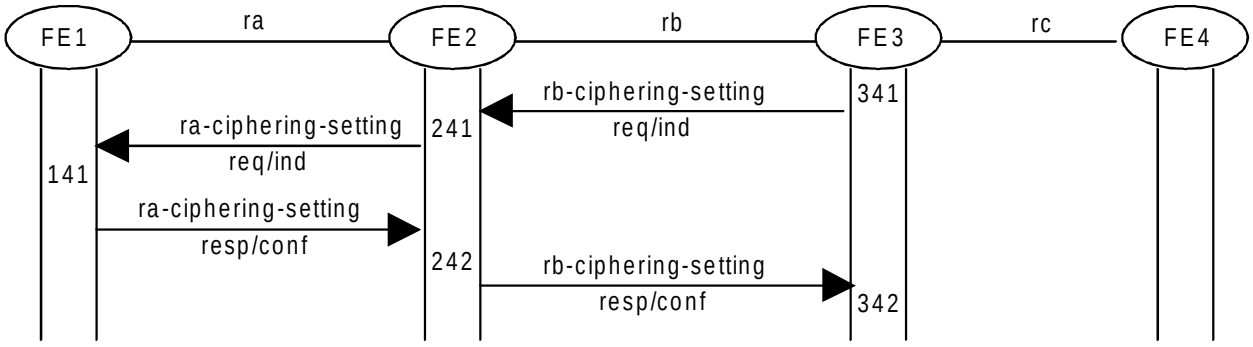
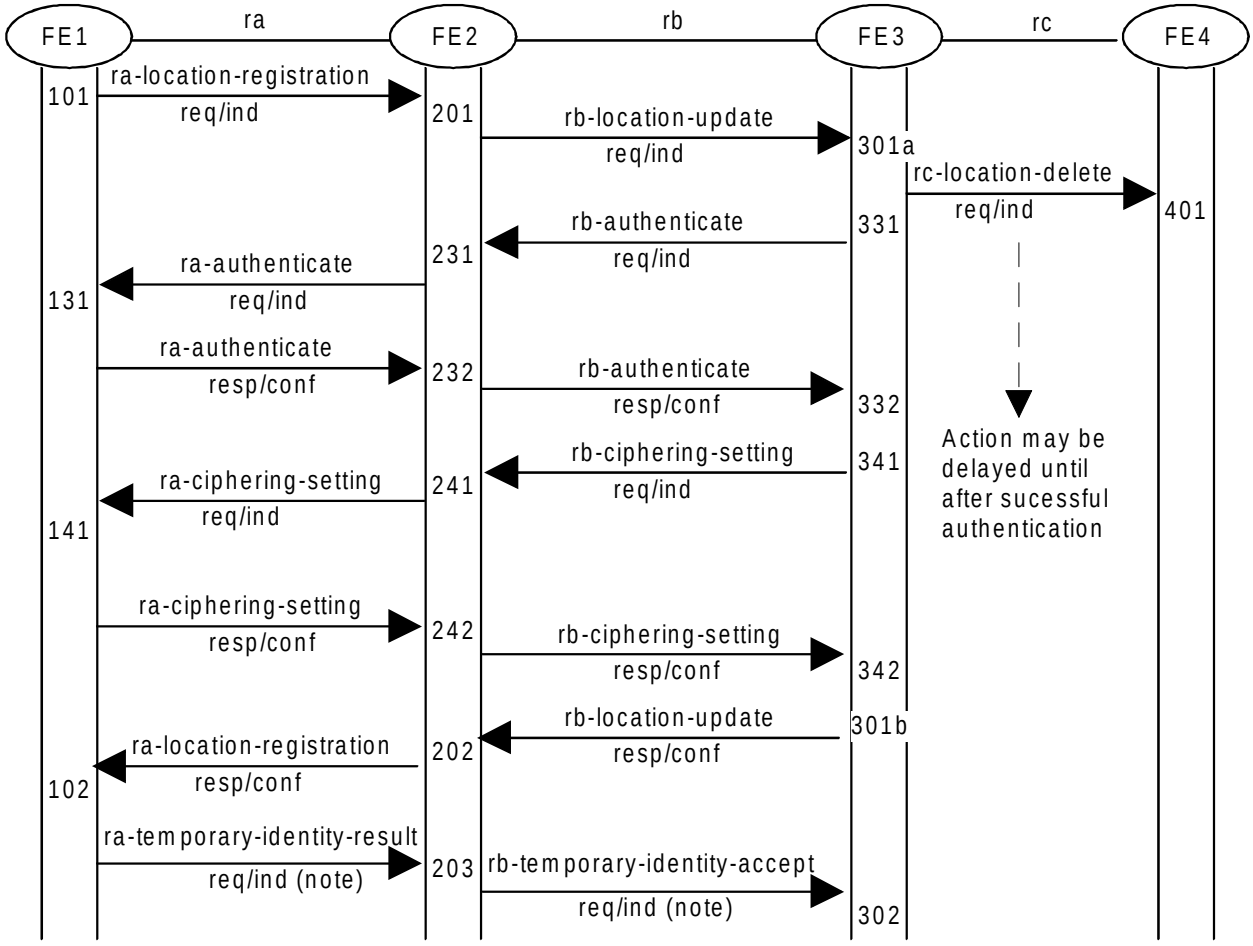


Figure 8: Normal operation of ciphering

Figure 9 shows a typical example of an overall information flow sequence for normal operation of MM features. Information flows for location registration, authentication, ciphering and temporary identity assignment may, but need not, occur in this order.



NOTE: ra/rb-temporary-identity-result/accept req/ind is only sent if the network had proposed a (new) temporary identity in ra-location-registration resp/conf.

Figure 9: Typical example of overall information flow sequence for normal operation of MM features

4.2.3.2 Exceptional operation of MM features

Only few examples of exceptional procedures are provided.

Figure 10 shows the information flow sequence for exceptional operation of authentication.

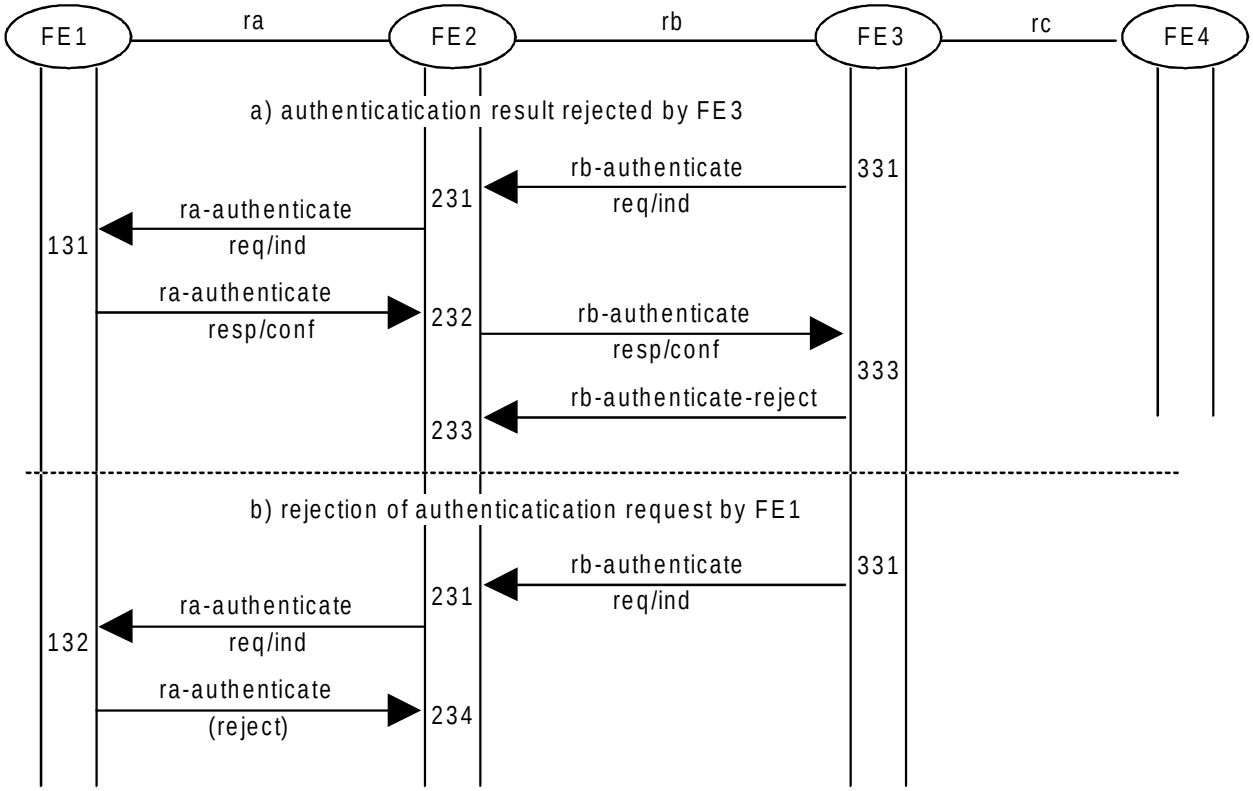


Figure 10: Exceptional operation of authentication

4.3 Functional entity actions

4.3.1 Functional entity actions of FE1

Actions for location registration, including assignment of temporary identities:

101 A location update is always initiated by FE1 and is always started as a location update in the DECT access network. FE1 can initiate a location update for one of the following reasons:

- normal location update: a change of DECT location area is detected by FE1 (old DECT location area identity stored in FE1 is different from a new encountered DECT location area identity);
- attach: after a period of detachment where the terminal was not able to receive incoming calls (e.g. because it was switched off), the terminal is now ready to again receive calls;
- location update as a result of an indication from FE2 that DECT location areas have been re-arranged.

NOTE: GSM does not support a similar possibility to inform the user that location areas have been rearranged.

Upon detection of a valid condition for DECT location registration, FE1 shall send an ra-location-registration req/ind to FE2.

102 On receipt of an ra-location-registration resp/conf, indicating that the location update has been accepted by the network, FE1 shall store the parameters received (DECT location area identification and, if available, the new temporary GSM identity). If a new temporary GSM identity was received, then FE1 will accept this assignment by sending ra-temporary-identity-result req/ind to FE2.

103 On receipt of ra-temporary-identity-assign req/ind from FE2, FE1 deletes the current temporary identity (if present). Then it assigns the new received temporary identity, unless no new temporary identity has been received (IMSI has been received instead). Then FE1 replies by returning ra-temporary-identity-assign resp/conf to FE2.

Actions for detach of the portable:

111 Upon explicit request from the user, or e.g. because FE1 detects a power off of the portable, FE1 reports to the network that the portable is inoperative by sending ra-detach req/ind to FE2.

Actions for identity requests by the network:

121 On receipt of ra-identity-request req/ind from FE2, FE1 replies by returning ra-identity-request resp/conf containing the requested identity.

Actions for authentication:

131 On receipt of ra-authenticate req/ind from FE2, FE1 shall perform the authentication algorithm and calculate the ciphering key. The calculated cipher key shall be associated with the received cipher key sequence number. The FE1 replies by returning ra-authenticate resp/conf containing the calculated authentication result.

132 If FE1 cannot accept the authenticate request, e.g. because it does not support GSM authentication, it shall respond with an ra-authenticate resp/conf, indication failure.

Actions for ciphering:

141 On receipt of ra-ciphering-setting req/ind from FE2, FE1 shall use the cipher key as indicated by the cipher key sequence number received from FE2. Then FE1 replies by returning ra-ciphering-setting resp/conf. This resp/conf is explicitly sent only in the case of a rejection. In case of acceptance it is sent indirectly via switching on the encryption at layer 2.

4.3.2 Functional entity actions of FE2

Actions for location registration, including assignment of temporary identities:

201 On receipt of ra-location-registration req/ind, FE2 performs the required procedures at a DECT access network level, i.e. registers the new location of the served user in the DECT access network coverage domain, maintains the information for the served user when that user first registers and deletes location information at the old visited DECT location if in the same domain and if necessary. FE2 also determines whether the initiating user has access to the global mobility service as described in this ETS. In order to enable FE2 to do that, FE1 provides FE2 with information, via ra-location-registration req/ind, on the subscription of the user (IPUI type "R" and/or on indication of the access rights). If the user is a user of the global mobility service, and if the previous visited location area was not in the domain of the current DECT access network, FE2 shall send an rb-location-update req/ind to FE3. FE2 shall perform the necessary mapping functions to provide FE3 with required information in the rb-location-update req/ind information flow.

202 On receipt of an rb-location-update resp/conf from FE3, FE2 will send an ra-location-registration resp/conf to FE1. If received from FE3, ra-location-registration resp/conf will include a temporary (global network) subscriber identity.

203 After receipt of ra-temporary-identity-result req/ind from FE1, FE2 sends rb-temporary-identity-accept req/ind to FE3.

204 After receipt of rb-temporary-identity-assign req/ind from FE3, FE2 sends ra-temporary-identity-assign req/ind to FE1.

205 After receipt of ra-temporary-identity-assign resp/conf from FE1, FE2 sends rb-temporary-identity-assign resp/conf to FE3.

206 The DECT access network may request the portable to initiate a location registration procedure by sending ra-location-update req/ind to FE1. This may be done e.g. after the DECT location areas have been re-arranged. Since there is no comparable feature defined for GSM, this procedure is further outside the scope of this ETS.

Actions for detach of the portable:

211 After reception of ra-detach req/ind, FE2 will disable any further calls towards the portable without sending a paging message on the radio path, until the portable attaches again to the network (by a location registration procedure). In addition, FE2 sends an rb-detach req/ind to FE3, to prevent also the global network from sending further incoming calls to the portable.

Actions for identity requests by the network:

221 After receipt of rb-identity-request req/ind from FE3, FE2 sends ra-identity-request req/ind to FE1.

222 After receipt of ra-identity-request resp/conf from FE1, FE2 sends rb-identity-request resp/conf to FE3. If the requested identity is not available in FE1 (empty parameter received from FE1), then no rb-identity request resp/conf shall be send to FE3. Actions for authentication.

231 After receipt of rb-authenticate req/ind from FE3, FE2 stores the received cipher key sequence number and then sends ra-authenticate req/ind to FE1.

232 After receipt of ra-authenticate resp/conf from FE1, FE2 sends rb-authenticate resp/conf to FE3 including the received authentication result.

233 On receipt of rb-authenticate-reject req/ind from FE3, FE2 shall regard the authentication of the user as failed.

234 On receipt of a ra-authenticate resp/conf from FE1 indicating a reject, FE2 shall regard the authentication as not successfully completed. No action is taken in the direction of FE3.

Actions for ciphering:

241 After receipt of rb-ciphering-setting req/ind from FE3, containing the actual cipher key for encryption, FE2 shall store and use this cipher key. Then FE2 sends ra-ciphering-setting req/ind to FE1, including the cipher key sequence number. This cipher key sequence number has either been received in a previous procedure from FE1 (DECT location registration, paging, PP initiated call establishment) or the value has been given from the FE3 during a previous authentication procedure. The latest previously received value is used.

242 After receipt of ra-ciphering-setting resp/conf from FE1 indicating acceptance, FE2 sends rb-ciphering-setting resp/conf to FE3. If ra-ciphering-setting resp/conf indicates a rejection, ciphering has not been switched on, in that case no action is taken in the direction of FE3.

4.3.3 Functional entity actions of FE3

This FE registers the new location of the served user in the GSM radio coverage domain, maintains the information for the served user when that user first registers in GSM domain and deletes location information at the old visited GSM location if necessary.

Actions for location registration, including assignment of temporary identities:

301a Upon receipt of rb-location-update req/ind, FE3 validates if the request can be accepted (e.g. whether roaming is allowed or whether the user is a legitimate global network user). If the request is accepted, the global network registers (HLR, VLR) will be updated conform the new location of the served user. And if applicable, FE3 should also inform FE4 (i.e. the previously visited DECT access network) that the served user is no longer in FE4's domain, by sending an rc-location-delete req/ind to FE4.

NOTE: Optionally FE3 may now initiate authentication and ciphering procedures first (this is described in separate FE actions) before continuing with actions 301b.

301b If the location update is accepted, FE3 shall sent a positive confirmation towards FE2 by sending an rb-location-update resp/conf to FE2. In case identity confidentiality is active (global network decision), FE3 will assign and include a new (global network) temporary subscriber identity to the served user.

302 On receipt of rb-temporary-identity-accept req/ind from FE2, FE3 shall consider the new temporary identity (TMSI) as valid or, if an IMSI was sent to the portable, considers the old temporary identity (TMSI) as deleted.

303 If the global network wants to assign a new temporary identity (TMSI) to the portable, without a location registration being currently performed, FE3 sends rb-temporary-identity-assign req/ind to FE2 containing a new temporary global identity and an identification of the location area in which the new temporary identity applies. Alternatively, FE3 can also request the portable to delete the temporary global identity without assigning a new one, by sending the portable's IMSI instead of a new TMSI.

304 On receipt of rb-temporary-identity-assign resp/conf from FE2, FE3 shall consider the new temporary identity (TMSI) as valid or, if an IMSI was sent to the portable, considers the old temporary identity (TMSI) as deleted.

Actions for detach of the portable:

311 After reception of rb-detach req/ind, FE3 will disable any further call requests towards the DECT access network for the portable concerned, until the portable attaches again to the network (by means of a location registration procedure).

Actions for identity requests by the network:

321 FE3 may use the identification procedure to request a portable to provide specific identification parameters to the global network, e.g. IMSI or IMEI. For that purpose FE3 shall send rb-identity-request req/ind to FE2 containing an indication of the type of information requested.

322 FE3 shall expect rb-identity-request resp/conf from FE2 containing the requested identification information.

Actions for authentication:

331 FE3 may use the authentication procedure to request a portable to provide the authentication result to the global network. For that purpose FE3 shall send rb-authenticate req/ind to FE2 containing a random number and a cipher key sequence number. The random number shall be used together with the stored authentication key when calculating the requested authentication result. The cipher key sequence number shall be stored by FE2 and shall be associated by FE1 to the calculated cipher key.

332 FE3 shall expect rb-authenticate resp/conf from FE2 containing the requested authentication result.

333 If FE3 receives the rb-authenticate resp/conf and detects a failed authentication, it shall inform FE2 on the failure by sending rb-authenticate-reject req/ind.

Actions for ciphering:

341 FE3 may use the ciphering procedure to request the encryption of the air interface. For that purpose FE3 shall send rb-ciphering-setting req/ind to FE2 containing the cipher key that shall be used to encrypt the air interface.

342 FE3 shall expect rb-ciphering-setting resp/conf from FE2 to confirm that encryption for the air interface has been activated.

4.3.4 Functional entity actions of FE4

Actions for location registration:

401 Upon receipt of rc-location-delete req/ind FE4 shall delete all temporary data of the served user and shall route all further calls to the user to the global network.

4.4 Functional entity behaviour

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

All Specification and Description Language (SDL) diagrams for functional entities are provided according to the general principles of ITU-T Recommendation Z.100 [9].

4.4.1 Behaviour of FE1

Figure 11 shows the normal behaviour of FE1 in the form of an SDL diagram. Input signals from the right and output signals to the right represent information flows from and to FE2. Input signals from the left and output signals to the left represent primitives from and to the served user.

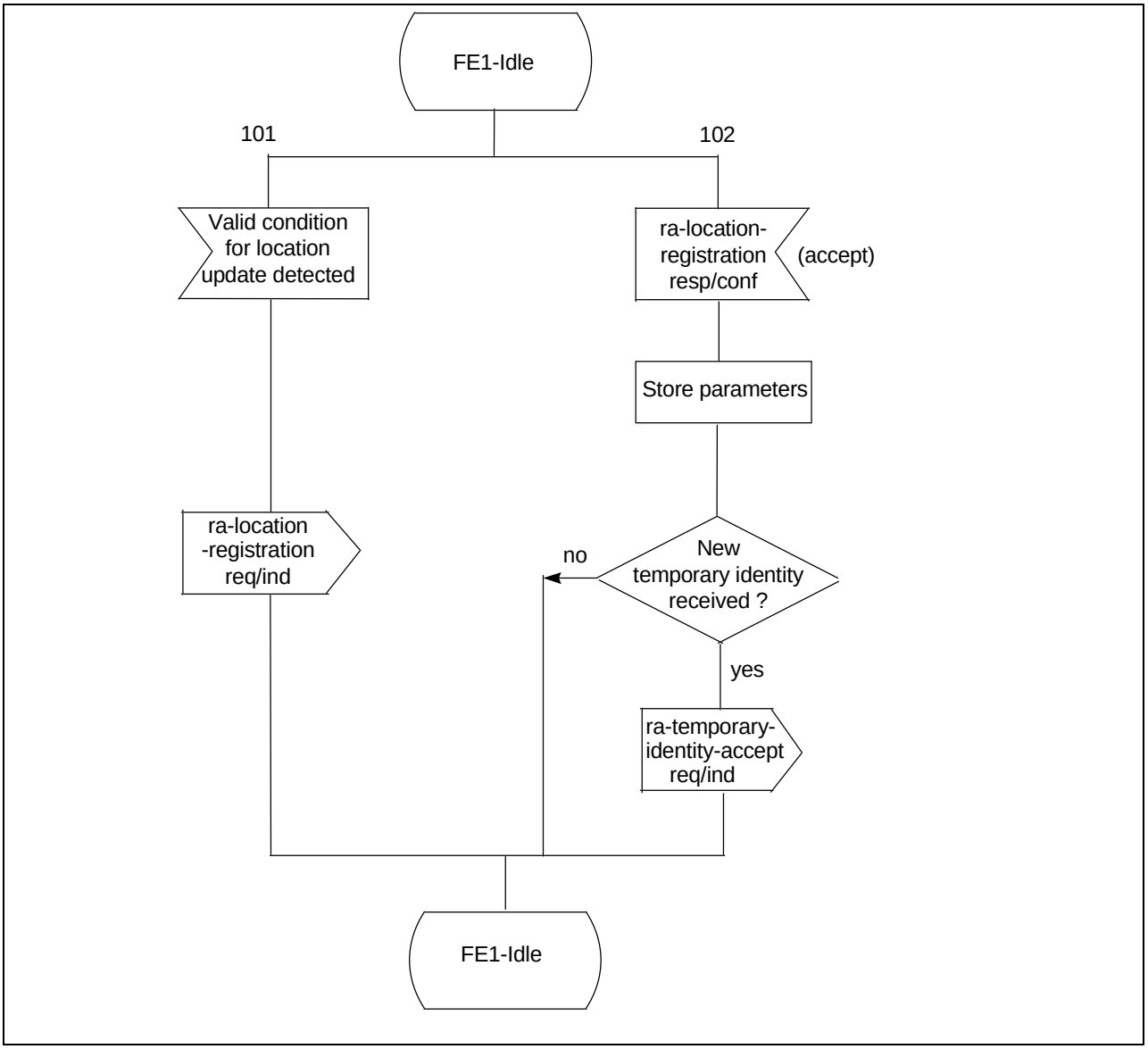


Figure 11 (sheet 1 of 3): MM - SDL for FE1

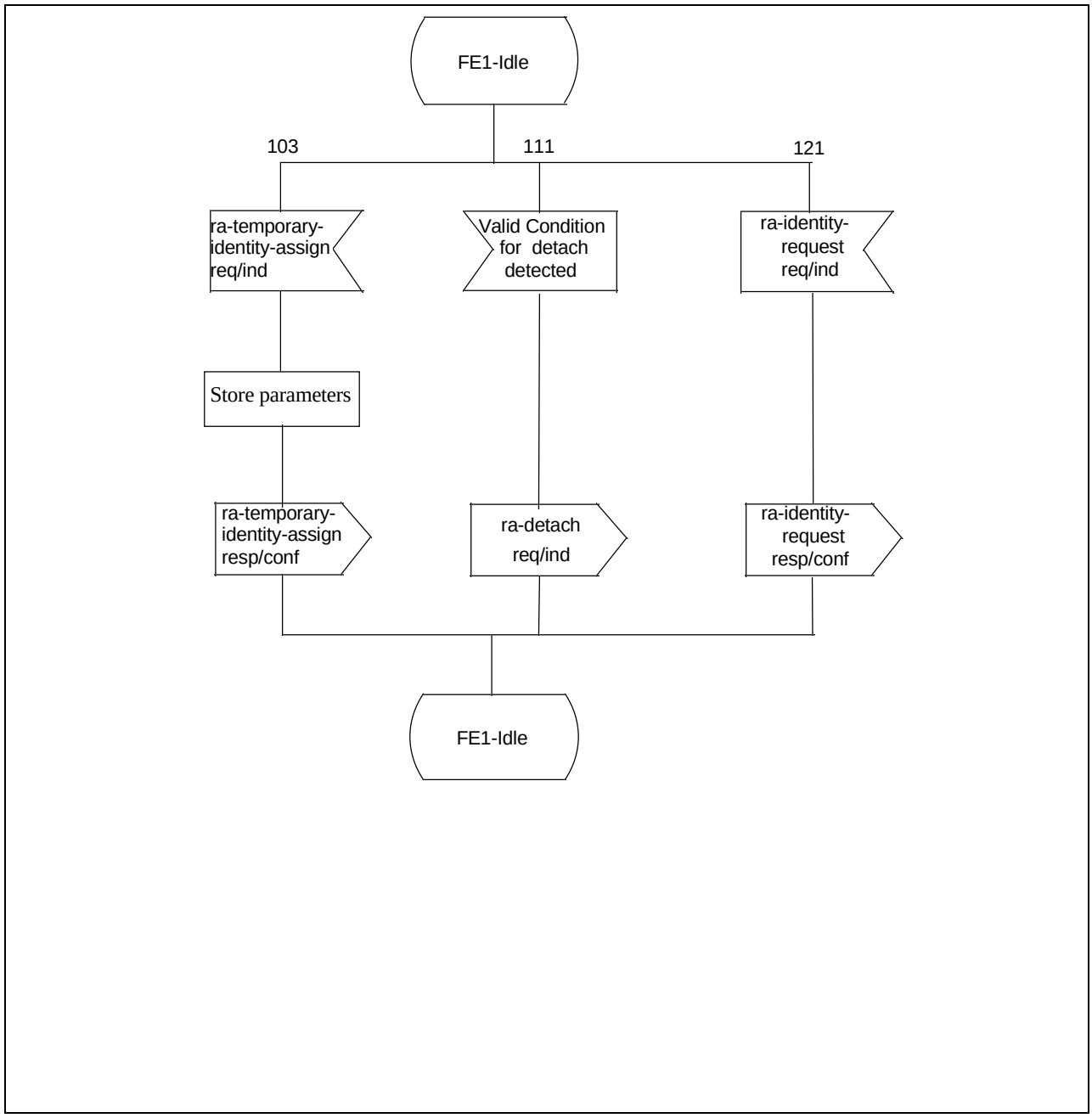


Figure 11 (sheet 2 of 3): MM - SDL for FE1

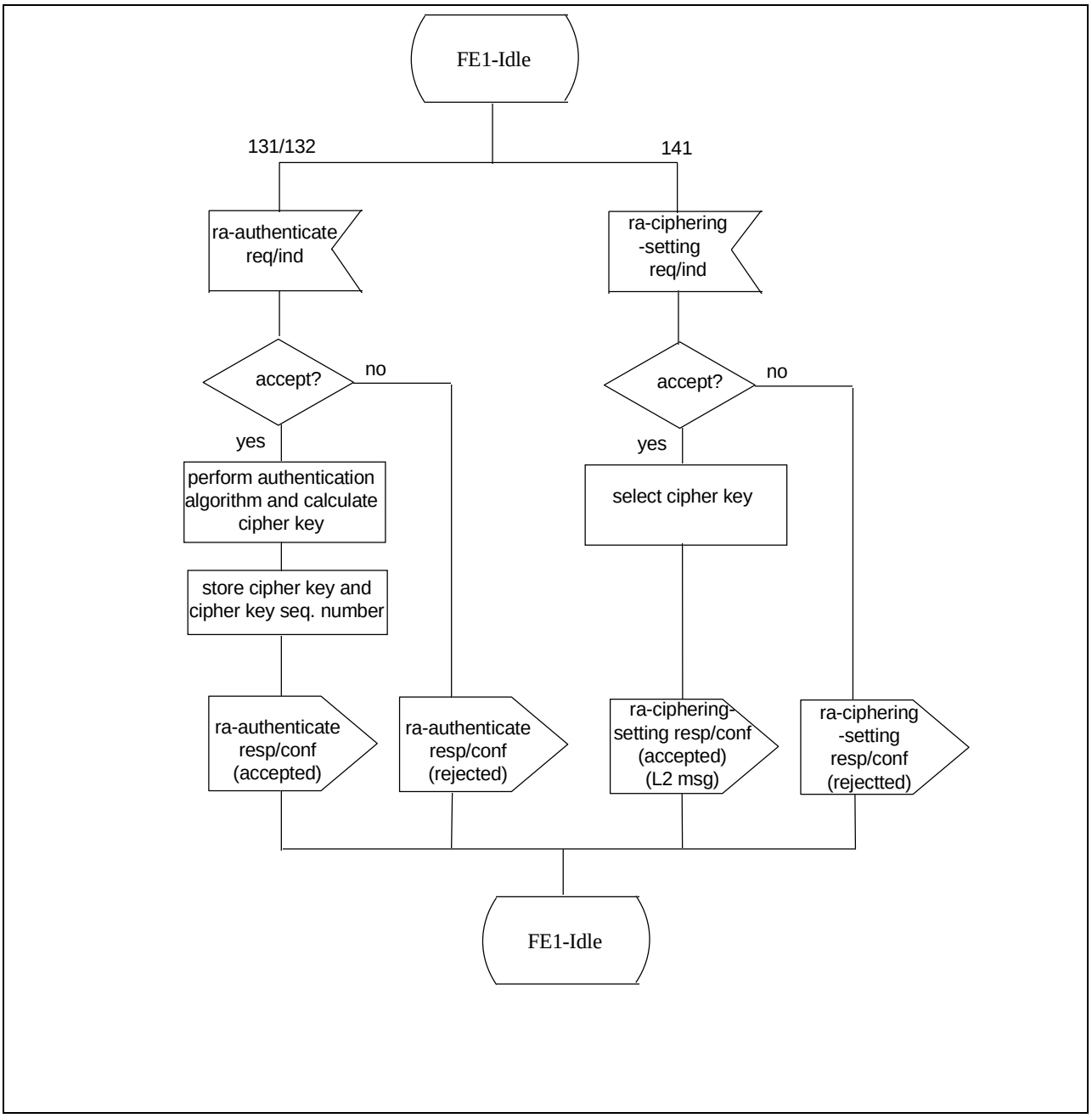


Figure 11 (sheet 3 of 3): MM - SDL for FE1

4.4.2 Behaviour of FE2

Figure 12 shows the normal behaviour of FE2 in the form of an SDL diagram. Input signals from the right and output signals to the right represent information flows from and to FE3. Input signals from the left and output signals to the left represent information flows from and to FE1.

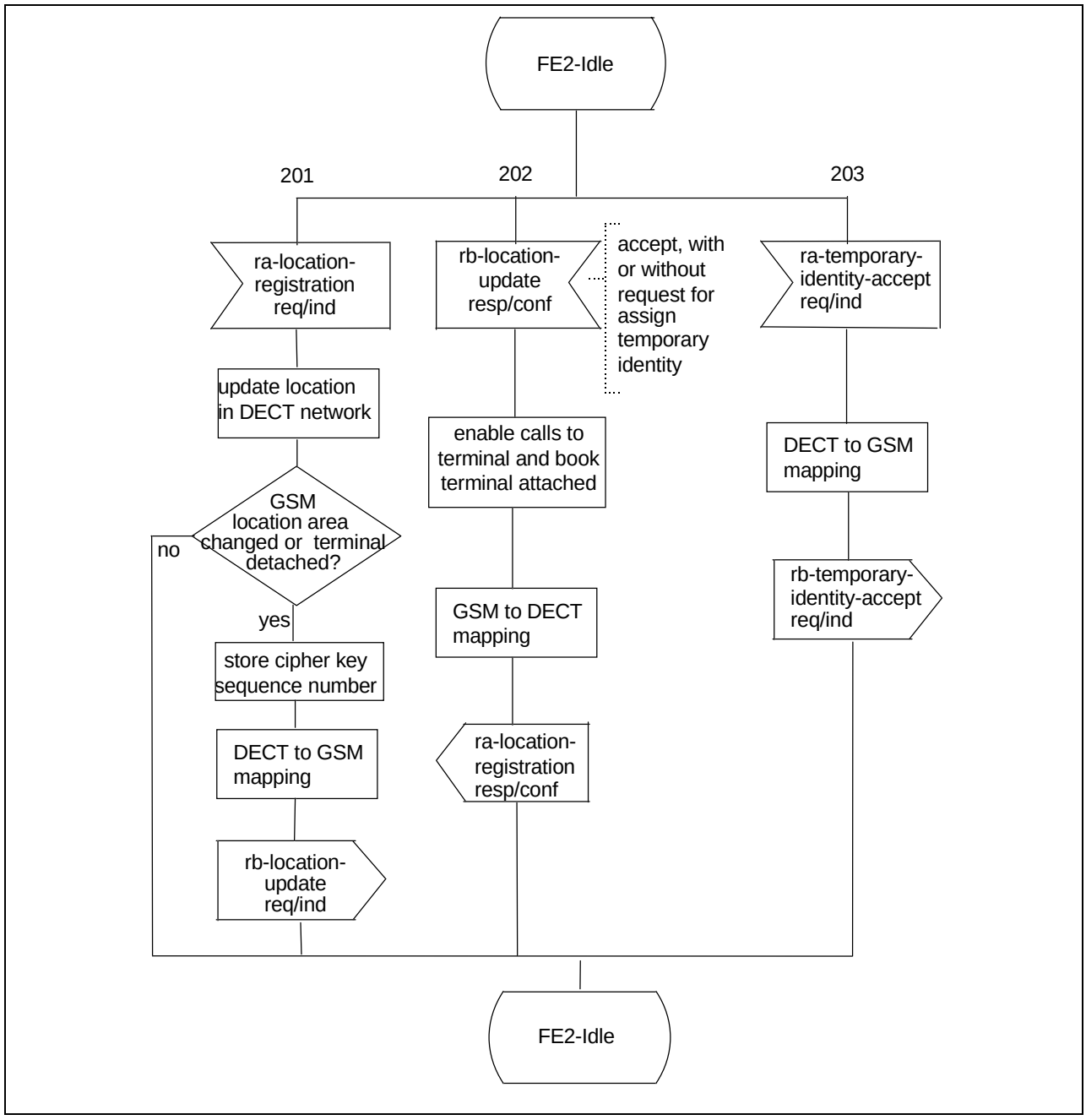


Figure 12 (sheet 1 of 3): MM - SDL for FE2

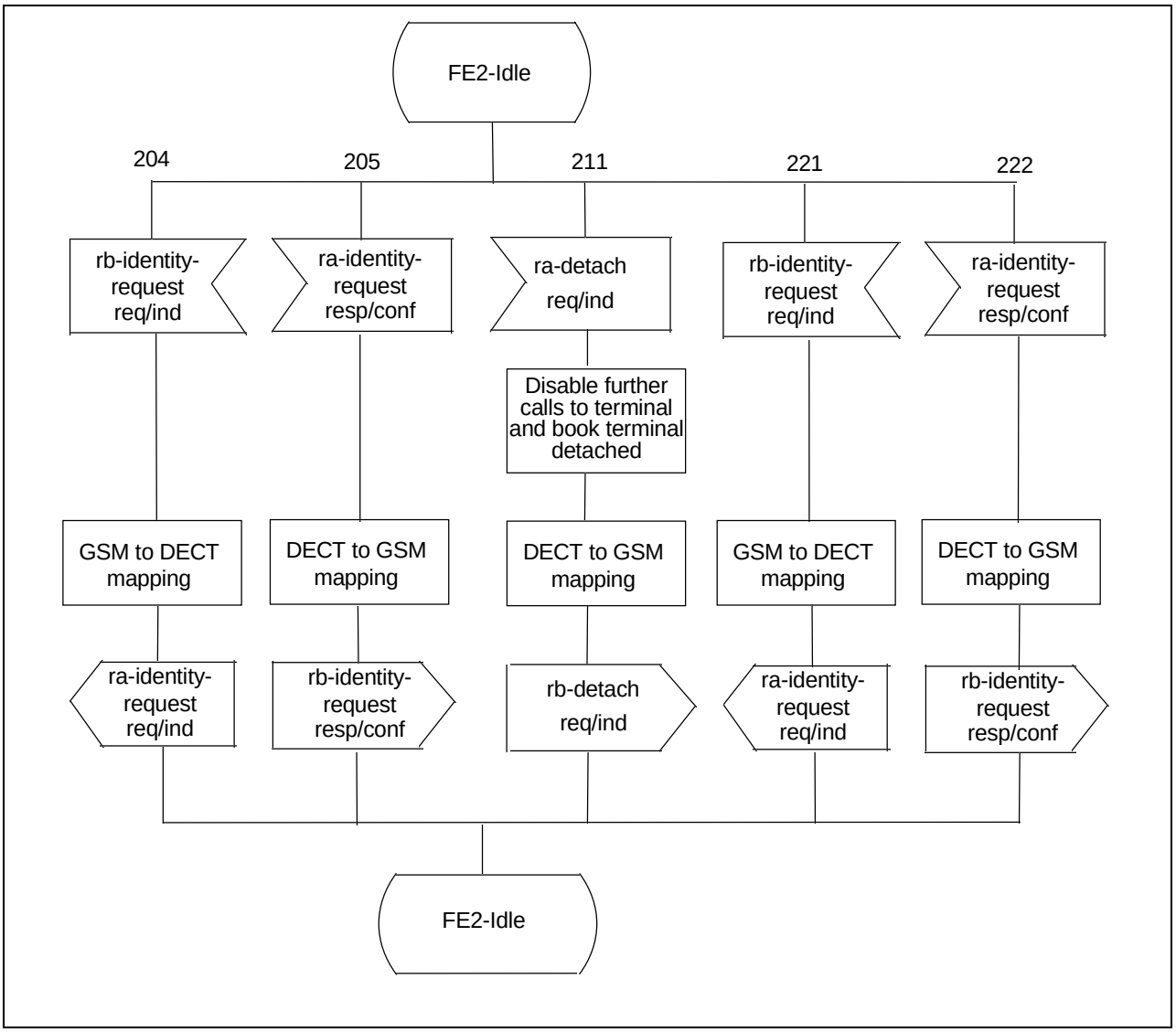


Figure 12 (sheet 2 of 3): MM - SDL for FE2

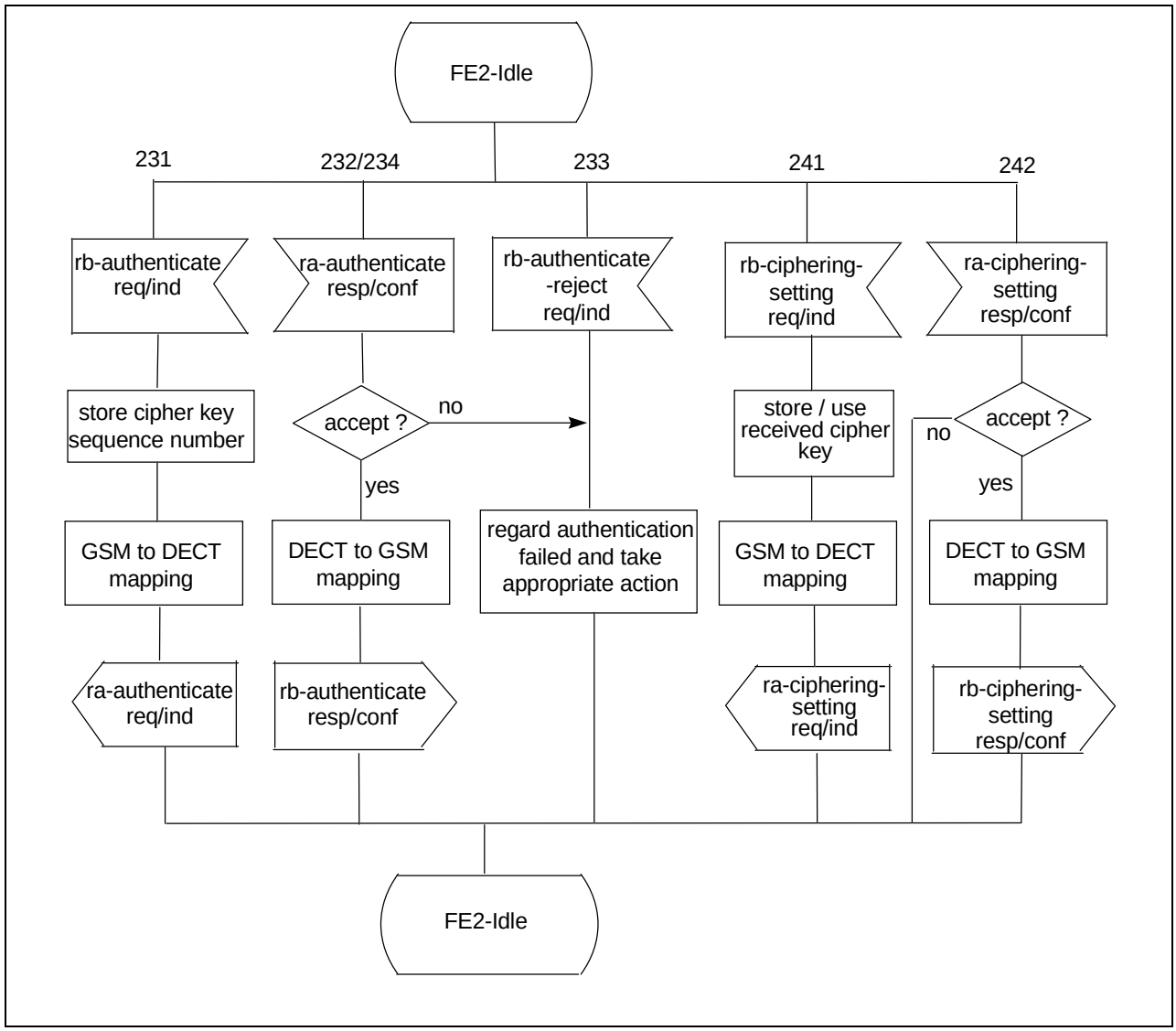


Figure 12 (sheet 3 of 3): MM - SDL for FE2

4.4.3 Behaviour of FE3

Figure 13 shows the normal behaviour of FE3 in the form of an SDL diagram. Input signals from the right and output signals to the right represent either primitives to an internal control entity in the global network, or information flows from and to FE4. Input signals from the left and output signals to the left represent information flows from and to FE2.

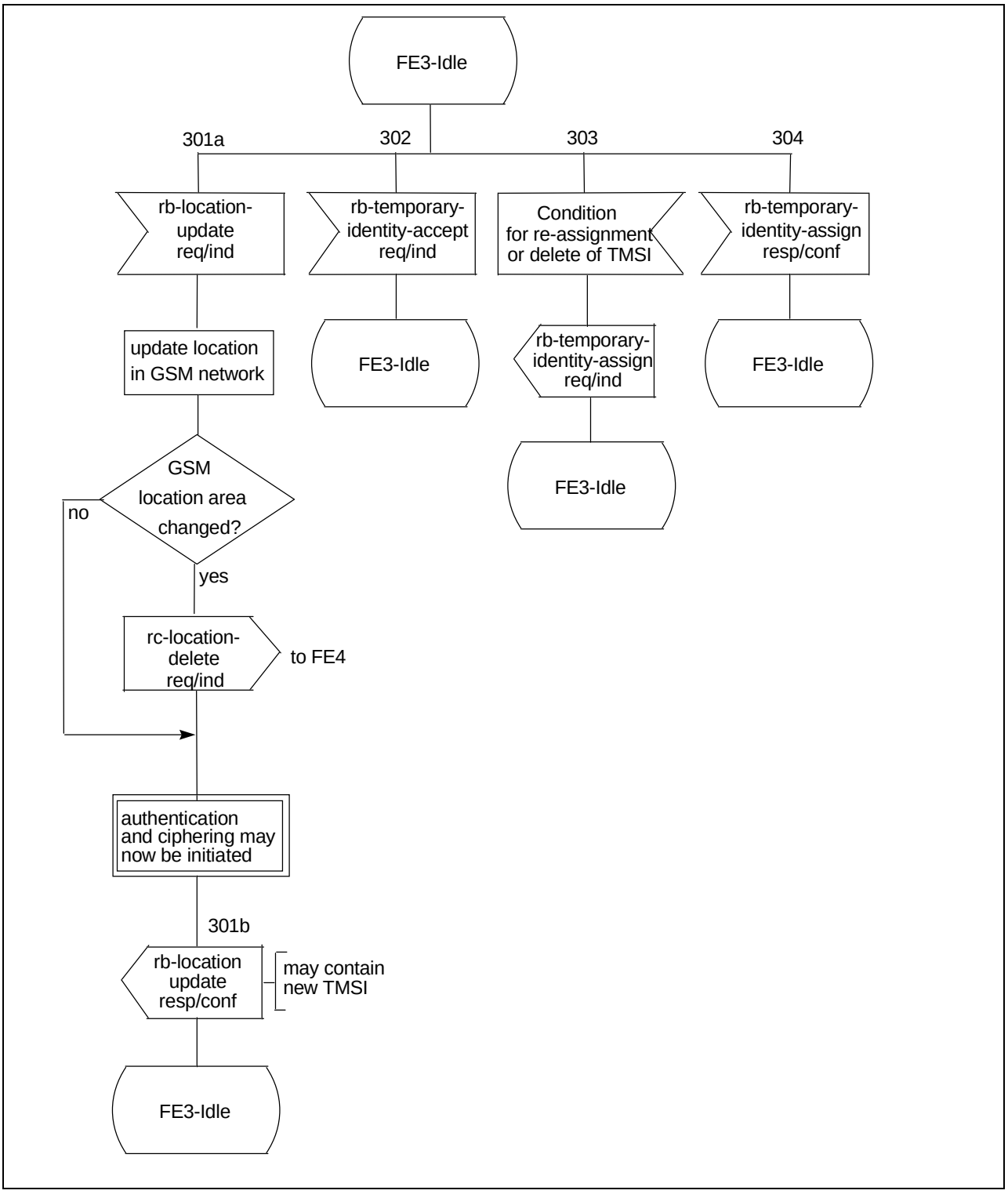


Figure 13 (sheet 1 of 3): MM - SDL for FE3

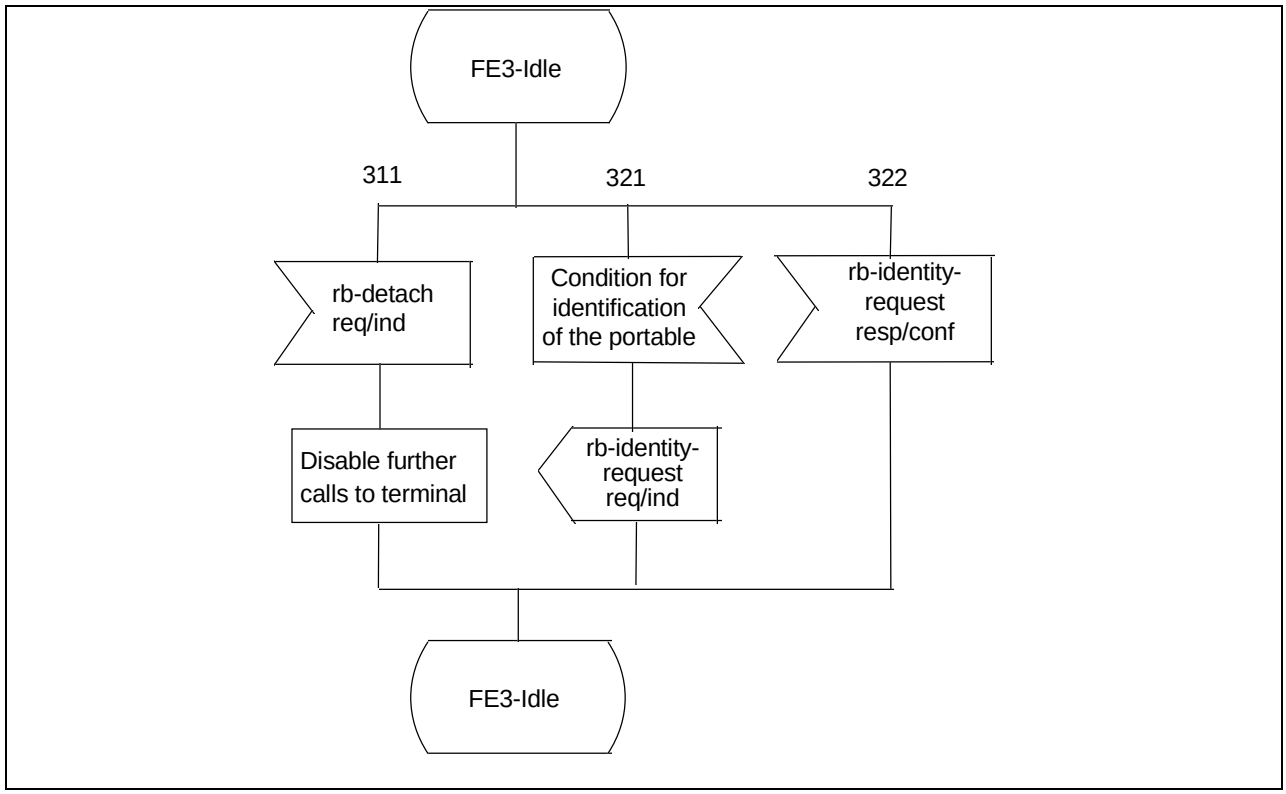


Figure 13 (sheet 2 of 3): MM - SDL for FE3

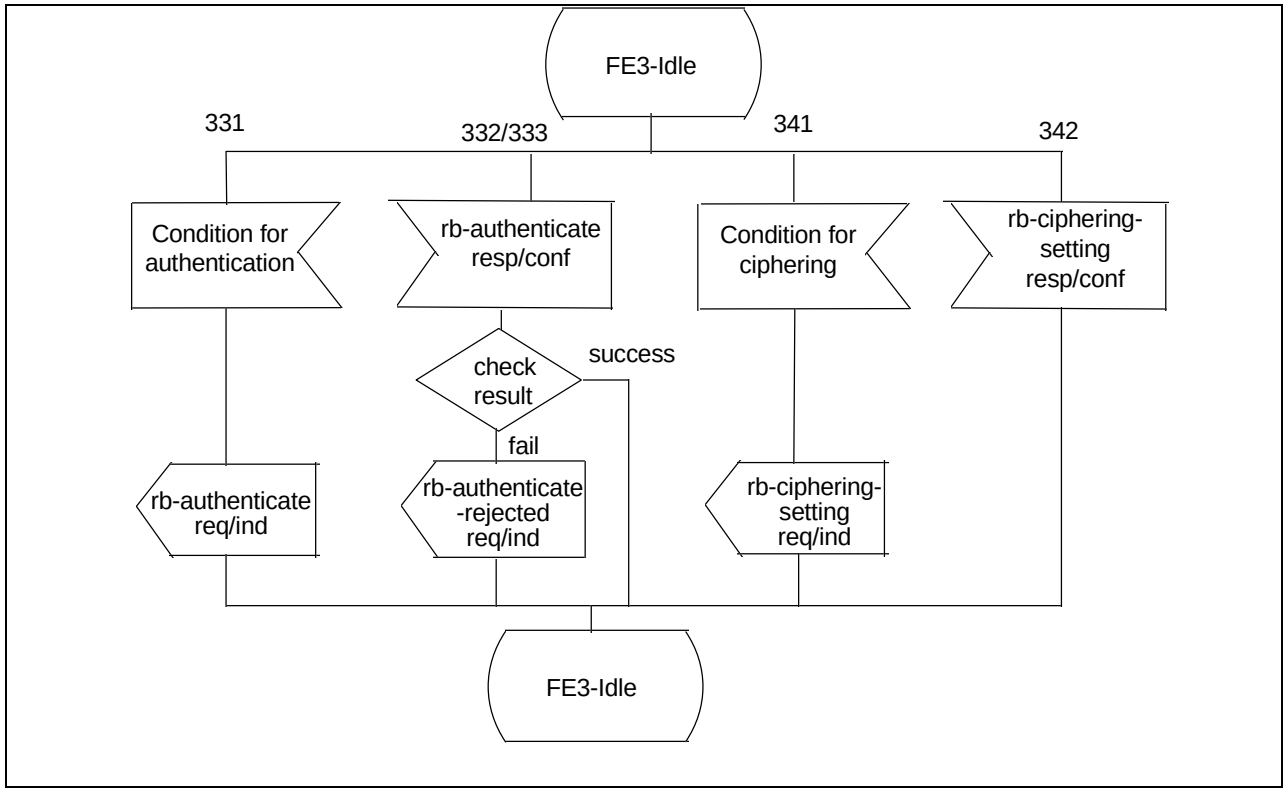


Figure 13 (sheet 3 of 3): MM - SDL for FE3

4.4.4 Behaviour of FE4

Figure 14 shows the normal behaviour of FE4 in the form of an SDL diagram. Input signals from the left and output signals to the left represent information flows from and to FE3.

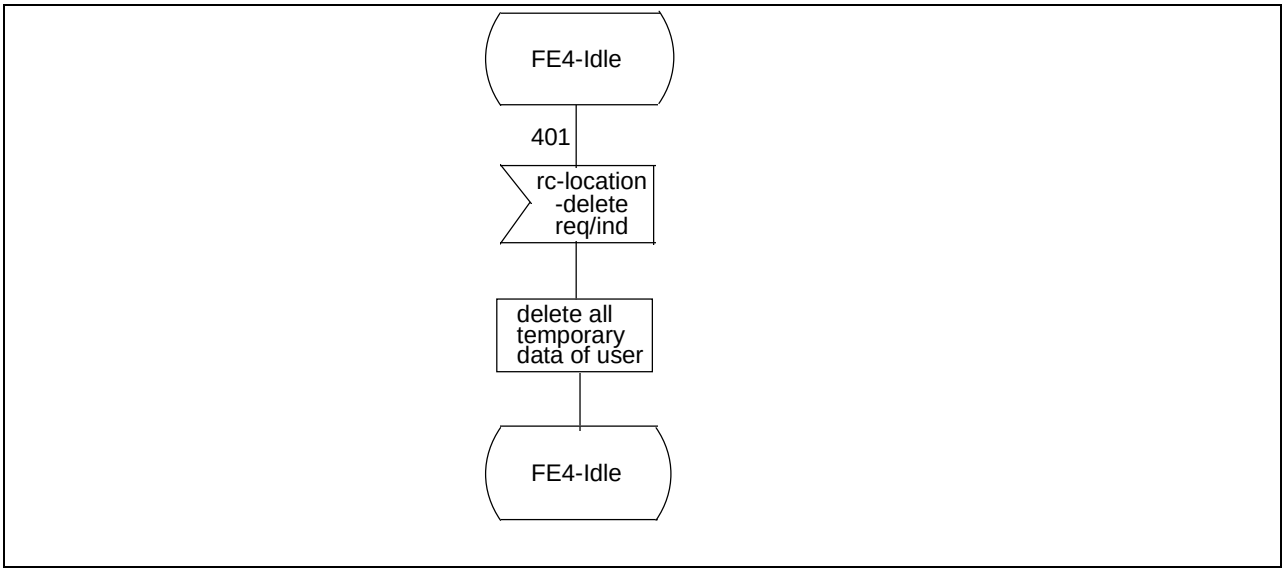


Figure 14: MM - SDL for FE4

4.5 Allocation of functional entities to physical equipment

A stage 3 standard for MM features shall be capable of supporting the allocations of FEs to physical equipment shown in table 15.

Table 15: Scenarios for the allocation of FEs to physical equipment

	FE1	FE2	FE3	FE4
scenario 1	DECT-PP	mobile user's currently visited DECT access network	GSM PLMN	mobile user's previously visited DECT access network
scenario 2	DECT-PP	mobile user's current DECT access network	GSM PLMN	-

4.6 Interworking considerations

DECT and GSM PLMN network elements have to cooperate in providing the service to the user. Some functions are allocated to the DECT part of the network, other functions are allocated to the GSM PLMN part of the network. The interworking between both sets of functions is described by the relationships between:

- FE2 and FE3 (relationship rb); and
- FE3 and FE4 (relationship rc).

This implies that information flows across rb and rc describe the required enhancements to the protocol over the ISDN interface between DECT and GSM networks. A stage 3 standard defining this interface and which conforms to this stage 2 standard shall take into account the coding requirements for information elements as defined for the GSM PLMN in ETS 300 557 [4] (GSM 04.08).

FE2 performs the required interworking functions for the mapping of the DECT and GSM information flows for MM. This mapping shall take into account the requirements defined in ETS 300 370 [3].

5 Call handling

5.1 Functional model

5.1.1 Functional model description

The functional model shall be as defined in ITU-T Recommendation Q.71 [5] and is reproduced in figure 15.

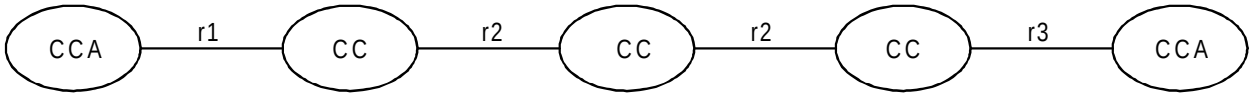


Figure 15: Functional model

The functional entities and functional relationships between these functional entities shall be as in ITU-T Recommendation Q.71 [5].

ITU-T Recommendation Q.71 [5] uses Functional Entities FE1 to FE5 in addition to the Call Control Agents (CCAs) and Call Controls (CCs). These have been omitted from figure 15, because they are not further used, and to avoid confusion with the FEs from the model for MM features.

5.1.2 Description of FEs

Shall be according to ITU-T Recommendation Q.71 [5].

5.2 Information flows

5.2.1 Definition of information flows

Shall be according to ITU-T Recommendation Q.71 [5] with the following additions:

- **SETUP req.ind and SETUP resp.conf**

  The additional items of information given in table 16 are, or may be, conveyed in the SETUP req.ind and SETUP resp.conf information flows.

Table 16

Use	Item	Relationship	req.ind	resp.conf
routeing info	Mobile Identity (IMSI, TIMSI)	r1, r2*, r2**, r3	mandatory	mandatory
originator info	Cipher key sequence number	r1, r2* (req.ind) r2**, r3 (resp.conf)	mandatory	mandatory
originator info	Emergency call	r1, r2*	mandatory	-

  There is no need to include specific information on the mobile terminal characteristics (as is done in GSM with the "mobile station class mark"), because the information is fixed for ISDN-based terrestrial connections.

5.2.2 Examples of information flow sequences

Shall be according to ITU-T Recommendation Q.71 [5].

5.3 Functional entity actions

Shall be according to ITU-T Recommendation Q.71 [5].

5.4 Functional entity behaviour

Shall be according to ITU-T Recommendation Q.71 [5].

5.5 Allocation of functional entities to physical equipment

A stage 3 standard shall be capable of supporting the allocations of FEs to physical equipment shown in table 17.

Table 17: Scenarios for the allocation of FEs to physical equipment

FEs				
scenario 1	TE + DECT access network	Global network (GSM-PLMN)		TE + DECT access network
scenario 2	TE + DECT access network		Global network (GSM-PLMN)	TE + DECT access network
scenario 3	TE + DECT access network	Global network (GSM-PLMN)		TE + DECT access network
scenario 4	TE + DECT access network		Global network (GSM-PLMN)	TE + DECT access network

NOTE: No distinction is made between TE and DECT access network. This is out of the scope of this ETS, as this ETS focuses on the requirements for interworking between DECT access network and GSM PLMN. Mapping between ISDN call control and DECT call control procedures is contained in ETS 300 434-1 [8].

TE: Terminal Equipment.

5.6 Interworking considerations

The interworking between the DECT and GSM networks can occur on either of the relationships r1, r2 and r3. Interworking on the relationships r1 and r3 imply the connection of a "simple" DECT system with no call control functionality. Interworking on the relationships r2 imply the connection of a DECT Private Automatic Branch Exchange (PABX) or a DECT Private Integrated Services Network (PISN).

History

Document history			
August 1996	Public Enquiry	PE 111:	1996-08-05 to 1996-11-29
April 1997	Vote	V 9724:	1997-04-15 to 1997-06-13