3GPP TR 23.867 V7.1.0 (2005-12)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Internet Protocol (IP) based IP Multimedia Subsystem (IMS) emergency sessions
(Release 7)

Keywords

3GPP, IMS, Emergency

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document is a temporary container for the architectural impacts on IM CN subsystem and on IP-Connectivity Access Network for establishing an emergency session via IM CN subsystem. The contents of this report when stable will be moved into 3GPP Technical Specification e.g. TS 23.002 [1], TS 23.060 [2] and TS 23.228 [3].

2 References

The following documents contain provisions, which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. IN the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 23.002: "Network Architecture".

[2] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2.

[3] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[4] 3GPP TS 23.003: "Numbering, addressing and identification".

[5] 3GPP TR 23.803: "Policy and Charging Control".

[6] 3GPP TS 23.271: "Functional stage 2 description of Location Services (LCS)".

[7] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[8] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".

[9] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

[10] 3GPP TS 25.331: "Radio Resource Control (RRC); Protocol Specification".

[11] 3GPP TS 25.413: "UTRAN Iu interface RANAP signalling".

[12] 3GPP TS 48.018: "Base Station System (BSS) - Serving GPRS Support Node (SGSN); BSS GPRS Protocol (BSSGP)".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 and the following abbreviations apply:

PSAP	Public Safety Answering Point

4 Overall architecture for IP based Emergency services

4.1 Architecture principles

4.1.1 Requirements for IMS Emergency Sessions

The solution for emergency sessions in the IMS shall fulfil the following capability requirements:

1. A CS capable UE shall use the CS domain for emergency services, if it is not explicitly guided by the network operator to use the PS domain.

2. It should be independent from the used underlying IP connectivity network with respect to the detection and routing of emergency sessions. This includes the support for cellular access network, and fixed broadband access amongst others.

3. Any kind of emergency numbers, all kinds of emergency SIP URIs and special indications for emergency sessions within the SIP signalling must be supported (especially IETF proposals on addressing should be taken into consideration).

4. Emergency sessions should be prioritized over "ordinary" sessions by the system.

5. Setup of IMS emergency sessions shall be possible for users with a barred public user identity.

6. The primary solution shall be that the UE can detect an emergency session (e.g. by evaluating the SIP-URI or the dialled number) by itself and indicates the emergency session to the network. But the specification must also support cases where the UE can't detect an emergency session.

7. The solution must work in case the UE has a UICC card and is registered to the IMS or not, as well as in the UICC-less case. In the UICC-less and non-registered cases it must be possible to setup a bearer in the IP connectivity network and session setup must be possible without an existing security association between UE and P-CSCF.

8. It must be possible to reject requests of an UE without UICC to establish bearer resources and attempts to make emergency sessions in networks where UICC-less emergency calls are not to be supported.

9. Emergency Service is not a subscription service and therefore will normally be supported entirely in the visited network and provided without interaction with a "Home" network in a roaming case, whether or not the UE is registered. The CSCFs providing service for emergency sessions may be different from the CSCFs involved in the other IMS services.

10. If an emergency session establishment request is routed via a P-CSCF located in the home network, the home network should be able to detect that the session is for emergency service (whether indicated as such or not) and respond to the UE indicating that the UE should initiate an emergency session in the visited network (e.g. via the CS domain of the visited network).

11. Emergency centers and PSAPs may be connected to the PSTN, CS domain, PS domain or any other packet network.

12. Emergency centres and PSAPs shall be able to call back the user.

13. If supported, the visited network may download emergency numbers to the UE, using, for example, procedures as described in TS 24.008 or other procedures provided by the used access network, in order to ensure that local emergency numbers are known to the UE.

14. For GPRS access a globally dedicated APN shall be used to indicate emergency access to PS domain.

15. The IMS core network shall be able to transport information on the location of the subscriber.

The solution for emergency sessions shall also fulfil the following architectural requirements:

1. The architecture for Emergency Service should be driven by the specific capabilities requirements. Specification should minimize the changes to existing IMS architecture and procedures, and re-use existing IMS functional entities. However the specification should not be constrained by the existing functional entities.

2. The architecture should take into account that it may be possible to make emergency calls on other media than voice. It needs to take account support, for example, the deaf and hearing-impaired using a text phone that might generate information, for example, using IMS messaging procedures. There may also be a need to work with phones that attempt the emergency call as a video telephony call.

3. Emergency service delivery via the PS domain may benefit where only some dedicated GGSN are equipped for specialised emergency handling. Globally dedicated emergency APN may be configured in the SGSN and GGSN and provided to the UE in order to support emergency services over the PS domain based on the requirements defined in section 4.1.1.

4.1.2 Procedures for SIP Emergency Session Establishment

It shall be possible for the network to discriminate between emergency sessions and other sessions. This shall allow special treatment (e.g. with respect to filtering, higher priority, routing, QoS) o f emergency sessions.

If a visited network can support PS emergency service, the emergency session should be setup in the visited network whether or not UE is registered in IMS in the home network.

The P-CSCF in the visited or home network is the IMS network entity, which always detects an emergency session. The UE is informed about the P-CSCF address in the visited network when activating a PDP context for emergency use. The P-CSCF in the visited network should route the corresponding request to an S-CSCF in the visited network, which is able to handle emergency sessions. A P-CSCF in the home network should respond to the UE indicating that the UE should initiate an emergency session in the visited network (e.g. via the CS domain of the visited network). The P-CSCF checks whether an anonymous emergency session request, e.g. in the UICC-less case, is allowed. If such a request is allowed, no security association between UE and P-CSCF is established and the request is forwarded to an appropriate S-CSCF.

The S-CSCF shall route the emergency request directly to an emergency centre/PSAP or BGCF based on location information provided by the UE and additionally other information such as type of emergency service in the request. If the request is destined for a BGCF, the S-CSCF shall translate the received SIP-URI or Tel-URL based on location information and additionally other information such as type of emergency service into a number, which is routable in the PSTN or CS domain. This routable number is forwarded to the BGCF and should have the same format as used for CS emergency calls. If required by regulations, determination of the emergency centre or PSAP may also be based on location information provided by the network (e.g. Location Services).

4.1.3 Procedures for IMS Emergency Session Establishment

In order to establish an IMS emergency session the UE needs to have IP-CAN bearers to be used for IMS related signalling and for the media related to the emergency session. The network shall ensure that these bearers are only used by the UE in the context of IMS emergency sessions. In the GPRS case the GGSN may use filter rules applicable to the globally dedicated emergency APN to ensure that only certain IP addresses (e.g. IP address of the Emergency CSCF) can be reached through the globally dedicated emergency APN.

4.2 Architectural considerations

4.2.1 Emergency Calls in absence of UICC

The following two subchapters describe two different options on how Emergency calls can be performed in absence of a UICC. The intention is to evaluate the two options and recommend one solution.

4.2.1.1 Emergency Calls in absence of UICC – simulated IMSI

When the UICC is not present or the UICC is not valid, the ME shall provide functionality of a UICC in order for the ME to obtain access to the GPRS system for emergency services, with the following default capability:

- Be able to generate an Emergency identity containing two primary fields as follows and the capability to enable the authentication and security procedures.
- One field, including a pre-defined tag (emergency PLMN identity (unique MCC + MNC); *editors note: MCC = 901, MNC = 008 have already been defined for use for emergency calls in GSM networks [4]*) to identify the identity as being an Emergency identity.
- A second field, that includes an identity generated from the IMEI (*Editor's note: for example, the least significant 9 digits of the IMEI excluding the spare digit*).

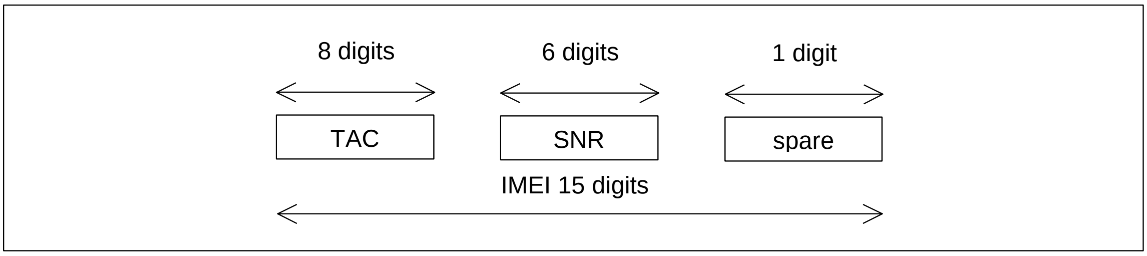

Figure 4.1: Format of IMEI

Emergency MCC	Emergency MNC	Random Digits based on IMEI

Figure 4.2: Example construction of emergency identity

On receiving an attach request with the emergency identity, based on the emergency PLMN id the network routes the necessary information to a HSS entity of the local operator that will provide the functionality of a home network for this user. The HSS functionality should allow the other network elements to handle the UICC-less emergency call no different from the case of a normal call.

The HSS/AuC can provide pre-defined authentication vectors for the ME, matching the functionality of the normal UICC-HSS pair and allow security procedures to be mimicked for the call as in the normal call establishment case. Security procedures can then be initiated at the network and mobile through use of pre-defined security key sets for integrity and ciphering. The pre-defined vectors are used by the SGSN and are static vectors in the ME and ciphering is started using the normal security procedures between the SGSN, RNC and ME.

Alternatively to the above mentioned method and to speed up the emergency call setup time a pre-defined emergency authentication vector can be stored in the SGSN. This authentication vector can be shared among all networks. In this case the SGSN shall not contact the HSS/AuC to retrieve authentication vectors.

After successful attach, the mobile shall continue with emergency session establishment.

The above method relies on the principle that using a simulated IMSI; the existing GPRS procedures can be reused without any major system impacts (including the UE). Additionally, the Mobile IMS application part should not be aware of the presence or absence of UICC. It should use the generated IMSI like the case of ISIM-less access and generate the appropriate IMPI/IMPU.

4.2.1.2 Emergency Calls in absence of UICC – use of IMEI

When the UICC is not present or the UICC is not valid, the ME shall identify itself in the Attach Request by the IMEI in the same way as in the CS domain (the CM Service Request).

NOTE: A UICC that is not valid is a UICC that in spite of being inserted is blocked for use, e.g. due to attempted accessed by a wrong pin-code or lack of roaming agreements.

As neither authentication nor ciphering functionality can be performed there is no need to communicate with any HSS. After successful attach, the mobile shall continue with emergency session establishment. For a detailed GPRS call procedure, see chapter 6.3.

The above ensures that the existing GPRS procedures can be used without any major system impacts both in the network and the UE

The UE shall not accept other numbers than the numbers stored in the ME as valid number for an emergency calls..

The emergency call application determines whether the CS emergency call or the IMS emergency call shall be used in the same way regardless whether the UICC is valid or not.

4.3 Security considerations

If the UE is equipped with an UICC, it shall be possible to authenticate the user and to provide integrity protection based on regulatory requirements.

If the UE is not equipped with an UICC, it shall be possible to grant access to the IP-CAN as well as to the IMS to enable the establishment of an IMS emergency session. As a consequence access is granted although the UE can not be authenticated and authorized by the access system or the IMS. In addition, the emergency communication can not be secured on the bearer and IMS layer, e.g. integrity protection between UE and P-CSCF is not possible.

4.4 General Packet Radio Service considerations

In GPRS, before IMS emergency session establishment, the UE performs an emergency attach if the UE is not attached to the network. The UE indicates the emergency attach by including an emergency indication to the Attach Request message. The network applies special treatment in case of the emergency attach procedure. After a successful emergency attach, only PDP context requests for emergency use shall be accepted by the SGSN. It is assumed that an already GPRS attached UE does not detach and re-attach for emergency services. If the UE is not equipped with an UICC, the UE performs the Emergency Attach using the IMEI or a simulated IMSI. In this case the SGSN checks whether such an anonymous Emergency Attach is allowed. If this is not allowed, the Emergency Attach is rejected.

At GPRS level the mechanisms for establishing a bearer for emergency use should not differ much from the normal GPRS bearer establishment currently specified by 3GPP. In fact there is only a need for the network to be able to detect the emergency use and to be able to give special treatment to these bearers.

As a minimum emergency sessions and bearers for them should not be dropped, so emergency bearers may require enhanced QoS, e.g. higher priority than subscription based priority.

The UE establishes a bearer for emergency use by including the globally dedicated emergency APN during PDP context activation. PDP context modification and PDP context deactivation procedures are not affected.

4.5 Radio network considerations

The emergency call setup over the PS domain should have similar priority mechanisms as emergency call setup in the CS domain.

The mechanism and priority of radio resources for channel allocation for the emergency session setup is FFS.

When the UE requests a signalling connection in order to perform an emergency attach or activate a PDP context with the globally dedicated emergency APN, it shall use a specific RRC (Radio Resource Control) establishment cause, see TS 25.331 [10] and TS 24.008 [9], annex L.

The detailed mechanisms and priority of radio resources for the media belonging to the emergency session is FFS. The radio access bearer of an activated PDP context for emergency use cannot be pre-empted, see TS 23.107 [8], TS 25.413 [11] and TS 48.018 [12]. The SGSN shall assign an appropriate allocation/retention priority to the radio access bearer.

4.6 Emergency location information and LCS functions

The S-CSCF routes the emergency request to the PSAP/Emergency Centre that corresponds to the current location of the UE. The access dependent variations of this approach are described below, for the cases where the UE is using GPRS, I-WLAN or fixed broadband access for the emergency service.

The S-CSCF forwards the SIP request containing the UE's location information to the PSAP/Emergency Centre. In this way, there is normally no need for the PSAP/Emergency Centre to request further information about the location of the UE.

4.6.1 Handling of emergency location information in GPRS

The UE shall include the cell identity as specified in [7], Annex B.3 in the SIP INVITE request, when it initiates an emergency session using GPRS bearer. It is noted that the UE normally is not aware of SAI and therefore SAI cannot be used as location information in SIP signalling.

In order to provide LCS information of a UE to an emergency centre or PSAP, the following procedure related to location services (LCS) may be used for emergency service.

At any time after detecting an emergency situation (i.e., after emergency Attach, Service Request for emergency, PDP context activation towards emergency APN or SRNS relocation or RAU towards a new SGSN), SGSN may initiate Packet Switched Network Induced Location Request (PS-NI-LR) procedure.

The existing network induced location procedure needs to be enhanced for the PS domain, following the same approach as in the CS domain. Otherwise the SGSN will not be able to push the location information of a terminal used for an emergency session to the appropriate emergency services client.

Figure 4.3 illustrates the enhanced network induced location request from the SGSN. The SGSN may initiate the Packet Switched Network Induced Location Request (PS-NI-LR) procedure as described below.

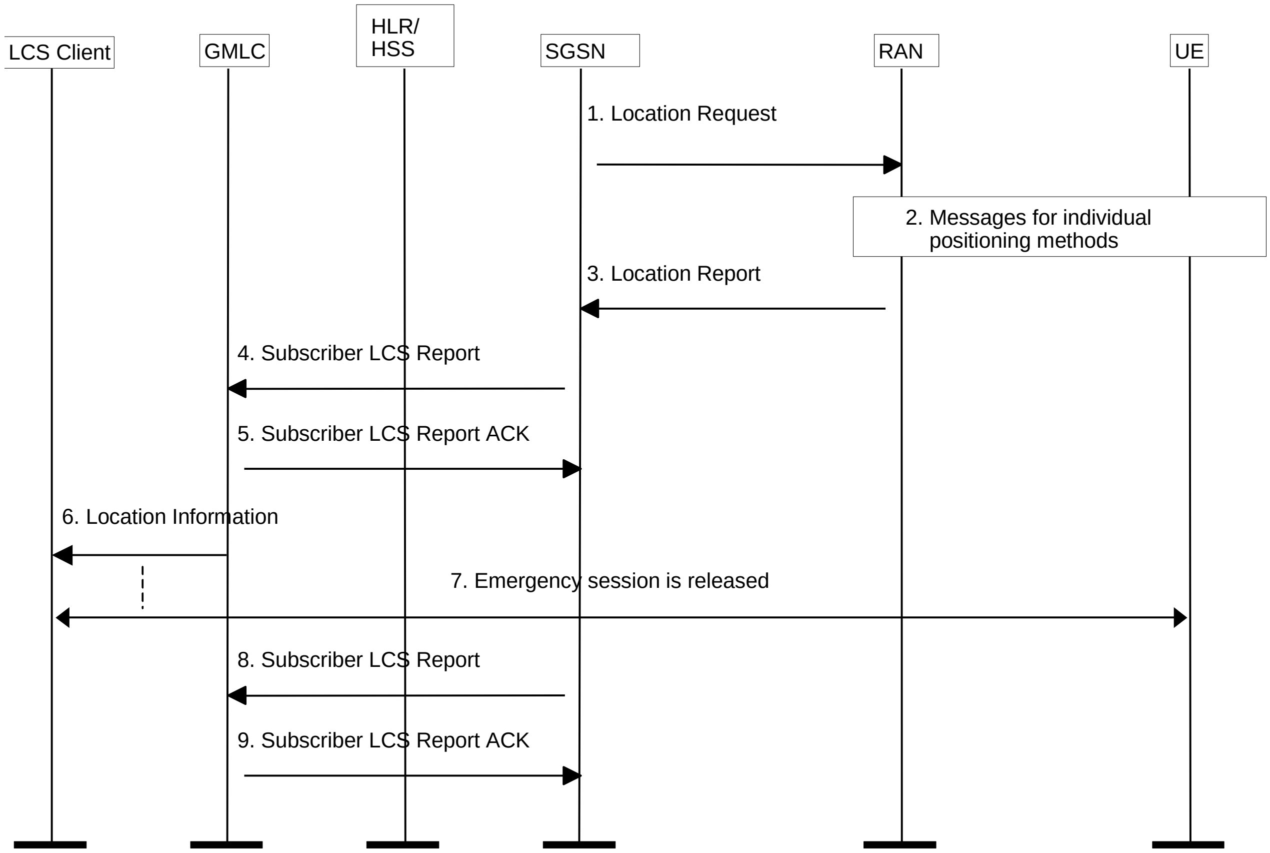

Figure 4.3: Positioning for a PS-NI-LR Emergency Service Session

1) After having detected an emergency situation, i.e. after emergency Attach, Service Request for emergency, PDP context activation towards emergency APN or SRNS relocation or RAU towards a new SGSN, the SGSN sends a Location Request message to the RAN. This message indicates the type of location information requested and requested QoS.

2) If the requested location information and the location accuracy within the QoS can be satisfied based on parameters received from the SGSN and the parameters obtained by the RAN e.g. cell coverage and timing information (i.e. RTT or TA), the RAN may send a Location Report immediately. Otherwise, the RAN determines the positioning method and instigates the particular message sequence for this method. If the position method returns position measurements, the RAN uses them to compute a location estimate. If there has been a failure to obtain position measurements, the RAN may use the current cell information and, if available, RTT or TA value to derive an approximate location estimate. If an already computed location estimate is returned for an UE based position method, the RAN may verify consistency with the current cell and, if available, RTT or TA value. If the location estimate so obtained does not satisfy the requested accuracy and sufficient response time still remains, the RAN may instigate a further location attempt using the same or a different position method. If a vertical location co-ordinate is requested but the RAN can only obtain horizontal co-ordinates, these may be returned.

3) When a location estimate best satisfying the requested QoS has been obtained, the RAN returns a Location Report to the SGSN with an indication whether the obtained location estimate satisfies the requested accuracy or not. This message carries the location estimate that was obtained. If a location estimate was not successfully obtained, a failure cause is included in the Location Report.

4) The SGSN determines the appropriate GMLC and emergency services client based on the received location estimate, SAI or cell identity. The SGSN shall send a MAP Subscriber Location Report to the GMLC carrying the MSISDN of the UE, the identity of the emergency services LCS client, the event causing the location estimate (PS-NI-LR), the location estimate and its age and the indication received from RAN whether the obtained location estimate satisfies the requested accuracy or not. The serving cell identity or SAI of the UE may be sent with the location information. The SGSN may record charging information.

5) The GMLC shall acknowledge receipt of the location estimate provided that it serves the identified LCS client and the client is accessible. The GMLC shall store the location information for later retrieval by the emergency services LCS client.

6) The GMLC may optionally forward the location information received in step 3 to the emergency services LCS client immediately. The GMLC may record charging information. The client is expected to obtain the location information by requesting it from the GMLC. The information about the positioning method used may be sent with the location information from the GMLC to the LCS client.

7) At some later time, the emergency services session is released.

8) The SGSN sends another Subscriber Location Report to the GMLC. This message may include the same parameters as before, except that there is no position estimate and an indication of emergency call termination is included.

9) The GMLC acknowledges the SGSN notification and may then delete all information previously stored for the emergency call per national regulation.

Editor's note: The identity used in PS-NI-LR may differ from the identity presented to the emergency centre or PSAP. This is FFS.

Editor's note: Steps 7-9 may be optional and are FFS.

As an alternative, Packet Switched Mobile Terminated Location Request (PS-MT-LR) procedure may be used for emergency service. No change is requested to the procedure itself, except PS-MT-LR location request will be initiated by emergency services LCS client through GMLC to the SGSN. The overall LCS procedure is described in the LCS stage-2 specification, see TS 23.271 [6].

4.6.2 Emergency location information for I-WLAN and fixed broadband access

For I-WLAN and fixed broadband access, the UE may already know its own geographical location and shall insert that information in the SIP INVITE request when establishing the emergency IMS session.

As an alternative, if the UE is not able to determine its own location, the UE should request its location from the access network, as described in Annex A, clause A.1.1. The access network determines the location of the UE and sends the location information to the UE. The UE shall insert the location information received from the access network in the SIP INVITE request. In this case the access network needs to maintain a database regarding the location of the terminal. If the UE does not know its location and is unable to obtain its location, then the terminal shall include an indication that its location is unknown in the emergency SIP INVITE.

It is an implementation issue on how the IMS network routes the emergency session based on location information. If the UE does not provide location information to the IMS network or the IMS network has to verify the provided location information, the IMS network may request location information from the access network, as described in Annex A, clause A.1.2. According to the implementation the IMS network may insert such location information in the emergency call set-up messages. That is, the IMS network will either insert the location information requested from the access towards the PSAP/Emergency Center or leave the location information in the SIP INVITE as given by the UE.

Editor's note: The format and content of the "location information" for fixed broadband and I-WLAN access is for further study but may be for example the street address or geographical coordinates.

4.7 High Level Procedures for IMS Emergency Services

4.7.1 UE Detectable Emergency Session

The following flow contains a high level description of the emergency service procedures performed when the UE can detect the emergency session is being requested.

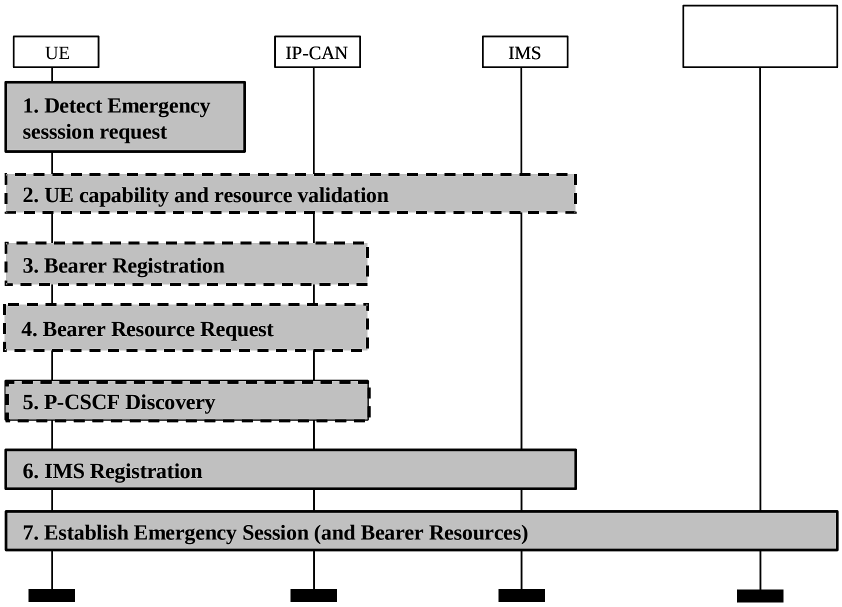
UE
IP-CAN
IMS
1. Detect Emergency sesssion request
2. UE capability and resource validation
3. Bearer Registration
4. Bearer Resource Request
5. P-CSCF Discovery
6. IMS Registration
7. Establish Emergency Session (and Bearer Resources)

Figure 4.4: Terminal Detected Emergency Calls

The following steps are performed:

1. The UE detects the request for the establishment of an emergency session.

2. In the case that the UE has insufficient resources or capabilities to establish an emergency call due to other ongoing sessions then the UE should terminate the ongoing communication and release reserved bearer resources. In the case of GPRS this implies e.g. to release a PDP context.

3. In the case that bearer registration is required and has not been performed, the UE shall perform bearer registration to the IP-CAN. In the case of GPRS, the bearer registration is the PS-attach procedure. If the UE is already registered or attached to the IP-CAN, then the bearer registration procedures are not required to be performed.
   Depending on the IP-CAN, the UE may be assigned an IP address at this stage.

4. In the case that bearer resources for the transport of the IMS related signalling are required to be reserved in the IP-CAN, the UE shall reserve the resources in the IP-CAN. The UE shall provide an indication that this is for an emergency service.
   In the case of a GPRS network, the bearer resource request procedure is the PDP context Activation Procedure, and a globally dedicated emergency APN is used as indication for an emergency request.
   If the IP-CAN does not provide an IP address to the UE in step 3, then the IP-CAN shall allocate an IP address to the UE during the bearer resource request procedures.

5. UE performs a P-CSCF discovery procedure, where the UE discovers a P-CSCF in the local network suitable for use in emergency sessions.

6. If the UE is equipped with an UICC, it shall initiate an IMS registration by providing the IP address obtained at step 3 or step 4 to the P-CSCF selected at step 5. The IP address used for signalling purposes is allocated in association with step 3 or step 4. The IMS registration request shall include an indication that this is for emergency services. This indication may be used to route calls coming from the PSAP to the contact address registered during the emergency registration procedure. Not to disturb established services the UE shall use a special emergency public user identifier in the emergency registration request.

   Note: The special emergency public user identifier is different from the emergency indication used in the IMS emergency registration request and IMS emergency session establishment request.

   When the network receives an IMS registration request with an emergency service indication the network should ignore roaming restrictions.

   The P-CSCF forwards the registration request to an appropriate emergency S-CSCF in the serving network. This S-CSCF forwards the registration request further on to the user's home network. Emergency registration requests are processed like any other registration requests. After successful registration the UE establishes a security association with the P-CSCF to provide for integrity protection between UE and P-CSCF.

   If the UE is not equipped with an UICC, it shall not initiate an IMS registration request, but instead immediately establish an emergency session towards the P-CSCF as described in step 7.

7. The UE shall initiate the IMS emergency session establishment using the IMS session establishment procedures containing an emergency session indication.

   - If the UE is equipped with an UICC, it shall send an IMS session establishment request to the P-CSCF containing an indication that this is for an emergency session establishment.

   - If the UE is not equipped with an UICC, it shall send an emergency session establishment request to the P-CSCF without prior registration. In this request the UE shall indicate that this request is coming from an anonymous user. When the P-CSCF receives an emergency session establishment request with an "anyonymous user" indication it shall check whether anonymous emergency sessions are allowed (e.g. UICC-less emergency sessions). In the case that anonymous emergency sessions are not allowed, and the "anonymous user" indication is present, the P-CSCF shall reject the session establishment request with sufficient information to inform the UE that the application level registration will not succeed. Otherwise the request is forwarded to an appropriate emergency S-CSCF although no security association between UE and P-CSCF is established.

   - Upon the reception of the emergency session initiation request, the S-CSCF shall route the signalling towards the emergency centre or the PSAP. The S-CSCF shall also route anonymous session establishment requests when the UE is not registered in the IMS.
     If the PSAP/emergency centre contains a point of presence within the IMS connectivity network, the S-CSCF shall forward the emergency session initiation request directly to the PSAP/emergency centre.
     If the PSAP/emergency centre has its point of presence in the PSTN/ISDN network or the CS domain, the S-CSCF shall forward the signalling to a MGCF (maybe via a BGCF). The MGCF will insert any available location information in the PSTN/CS signalling (this may require an additional location request enquiry).

Editor's note: The handling and structure of location information in the case of fixed broadband access is for further study.

Whether the procedures are activated individually by the UE or some of them are performed automatically depends on the implementation of the terminal and on the UE's configuration. For instance, the multimedia application in the UE could start the application level registration and steps 2-4 would have to be executed in response to support the operation initiated by the application. Interaction with the UE may happen during these steps.

4.7.2 Non UE detectable Emergency Session

The following flow contains a high level description of the emergency service procedures performed when the UE does not detect that the emergency session is being requested.

As the UE could not detect the emergency session, the session establishment request will be sent to the P-CSCF as per a normal session establishment procedure. Prior to send the session establishment request the UE must be registered in the IMS.

In the case that the P-CSCF can detect that that this is a request to establish an emergency session, then the following shall apply:

- Upon the reception of the session initiation request, the P-CSCF, upon detecting that this is an emergency request will reject the session initiation request with an indication that this is for an emergency session.

- When the UE receives the session rejection with the indication that the session initiation was for an emergency service, then the UE would initiate the "UE Detectable Emergency Session" described in sub-clause 4.7.1 above.

In the case that the P-CSCF does not detect that that this is a request to establish an emergency session, and the S-CSCF does detect that this is a request to establish an emergency session, then the following shall apply:

In the case that the subscriber is roaming:

- Upon the reception of the session initiation request without an emergency service indication, the S-CSCF, upon detecting that this is an emergency request will reject the session initiation request with an indication that this is for an emergency session.

- When the UE receives the session rejection with the indication that the session initiation was for an emergency service, then the UE would initiate the "UE Detectable Emergency Session" described in sub-clause 4.7.1 above.

In the case that the subscriber is at home:

- Upon the reception of the emergency session initiation request, the S-CSCF shall route the signalling towards the emergency centre or PSAP.
  If the PSAP/emergency centre contains a point of presence within the IMS connectivity network, the S-CSCF shall forward the emergency session initiation request directly to the PSAP/emergency centre.
  If the PSAP/emergency centre has its point of presence in the PSTN/ISDN network or the CS domain, the S-CSCF shall forward the signalling to a MGCF (maybe via a BGCF). The MGCF will insert any available location information in the PSTN/CS signalling.

5 Impacts on the UE and on the IM CN subsystem

5.1 UE

1. The UE should detect an emergency service request and indicate it to the network.

2. If the UE is CS capable and not attached to the PS domain, the UE shall attempt an emergency call in the CS domain. If the UE is only PS attached, and the network has indicated that IMS emergency services are supported, it should attempt the emergency call in the PS Domain. If the UE is attached to both domains, it should attempt the emergency call as directed by the network operator. No explicit direction means that the CS domain is the preferred domain for emergency calls. For an attempt in the IM CN Subsystem of the PS domain, the attempt should be in the serving (visited if roaming) IM CN Subsystem of the PS domain.

3. If the initial attempt is in the CS domain and it fails, the serving (visited if roaming) IM CN Subsystem of the PS domain should be attempted if the UE is capable.

   If the initial attempt is in the IM CN Subsystem of the PS domain and it fails, the UE should make the attempt in the CS domain (if the UE is capable and if for an appropriate service e.g., voice).

4. If #3 is not successful, or is not appropriate (e.g., visited PS domain does not support required PS emergency service), the session may be attempted in the Home IM CN Subsystem of the PS domain.

5. If a UE attempts to initiate a session and receives a 380 (Alternative Service) response with the type set to "emergency", the UE should then re-attempt the session as indicated in steps 2, 3, and 4, with first attempt being towards the CS domain (if the UE is capable and if for an appropriate service e.g., voice), and with an indication that emergency service is requested.

6. Other general requirements of UE refer to the general requirements of emergency calls in TS 22.101.

7. If the UE is not equipped with an UICC, it shall not initiate an IMS registration but immediately establish an emergency session towards the P-CSCF with an indication "anonymous user".

8. The UE shall use a special emergency public user identifier in the emergency registration request. The format of this public user identity has to be defined by stage 3.

The UE initiates the emergency session establishment request, and for the purpose of processing the request properly in the network the following specific information is supplied in the request message. These are not exhaustive information and the exact forms or values should be standardized in stage-3 work.

- Emergency session indication.

- Globally dedicated emergency APN.

- Optionally, type of emergency service. It could be implied in the above emergency session indication.

- UE's location information (e.g. Cell Global Identification for GPRS, other access networks may provide different types of location information).

5.2 IMS Functional entities

5.2.1 Proxy-CSCF

- Handle registration requests with an emergency indication like any other registration requests and forward such a request to the emergency S-CSCF.

- Detect an emergency session establishment request.

- On receipt of an unmarked session establishment request, which is recognized to be for an emergency service, the P-CSCF shall respond with a 380 (Alternative Service) with the type set to "emergency".

- On receipt of a marked emergency service session establishment request, the P-CSCF shall select an S-CSCF in the same network to handle the emergency session request and forward the request to that S-CSCF for further processing. The selection method is not standardized in the present document.

- On receipt of a session establishment request with an "anonymous user" indication, the P-CSCF shall check whether anonymous emergency requests are allowed. If such requests are not allowed, the request is rejected with an appropriate response.

5.2.2 Serving-CSCF

Emergency Registration procedures:

- In the roaming case, upon receiving a registration request with an emergency indication, forward the request to the user's home network.

- In the roaming case, upon receiving a response to an emergency registration request, forward the response to the P-CSCF.

Emergency Session establishment procedures:

- Receive an emergency session establishment request from a P-CSCF.

- Route emergency session establishment requests to an appropriate destination (e.g. PSAP/emergency centre or BGCF) based on location information and additionally other information such as type of emergency service in the request.

- The S-CSCF shall route anonymous session establishment requests when the UE is not registered in the IMS.

- If the emergency request has to be routed to an emergency centre or PSAP in the GSTN (PSTN or CS domain), translate the received SIP-URI or Tel-URL based on location information and additionally other information such as type of emergency service in a number that is routable in the GSTN. Forward the request including this number to a BGCF. This number shall have the same format as used for CS emergency calls.

Based on operator policy, the S-CSCF may respond to the emergency session request from the UE with indication to establish the session in the CS Domain.

5.3 Procedures for IP multi-media sessions

5.3.1 Emergency session establishment

This subclause presents the detailed session flows to establish an emergency session while at home or roaming. These flows assume the use of the optional Policy and Charging Control (PCC), which is described in TR 23.803 [5].

5.3.1.1 PSAP/Emergency center connected via IP using SIP

The following emergency session flow assumes a scenario when an emergency center or PSAP has IP connectivity and behaves as a SIP user agent.

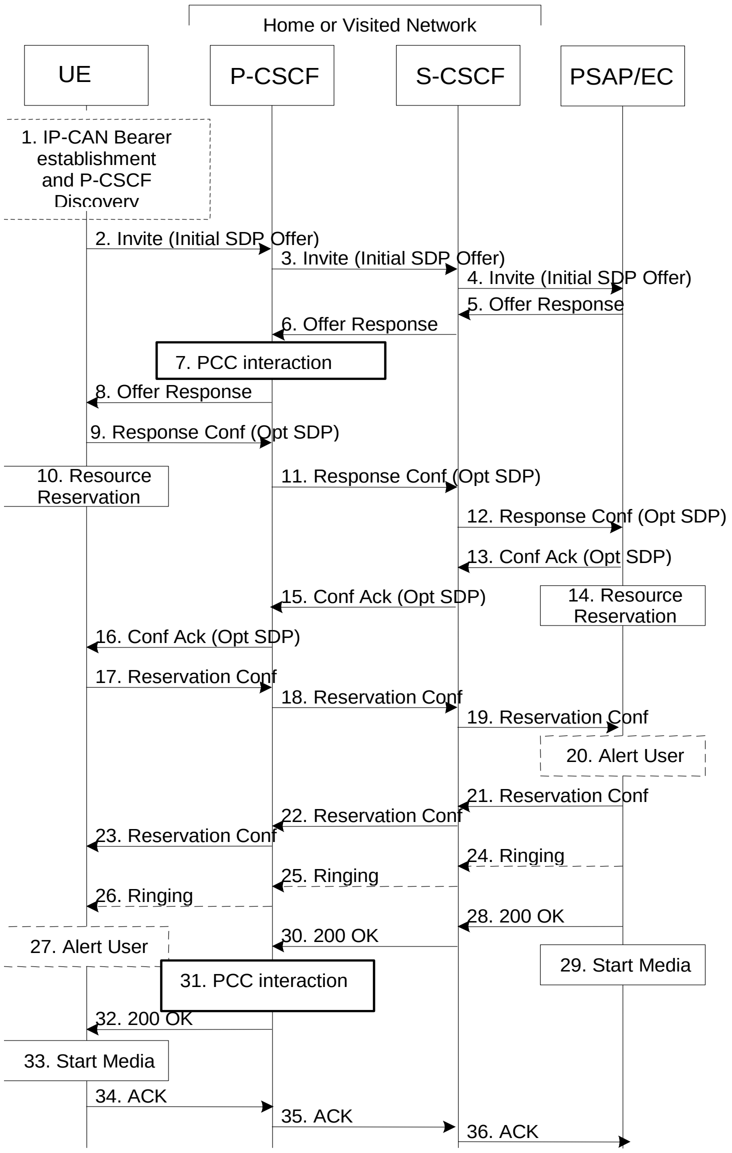

Figure 5.1: Emergency session establishment – emergency center/PSAP that supports SIP

1. In order to establish an IMS emergency session the UE must have an IP-CAN Bearer to be used for IMS related signalling and must have discovered a P-CSCF. P-CSCF discovery should use the PDP Context Activation mechanism where the P-CSCF address is sent to the UE in the Activate PDP Context Accept message.

2. UE sends the SIP INVITE request, containing an initial SDP, to the P-CSCF. The initial SDP may represent one or more media for a multi-media session. The SIP INVITE shall contain location information and it shall contain an emergency session indication when the UE has detected the emergency session itself.

3. When the P-CSCF receives an emergency SIP INVITE request it forwards the SIP INVITE request to a pre-configured S-CSCF in the same network. If an emergency indication was not set by the UE, then the P-CSCF returns a 380 (Alternative Service) response with the type set to "emergency".

4. The S-CSCF uses the location information to identify the correct PSAP or emergency center. The S-CSCF then forwards the request towards the PSAP / emergency center including the location information.

5. The PSAP/emergency center determines the subset of the media flows proposed by the originating endpoint that it supports, and responds with an Offer Response message back to the originator. The SDP may represent one or more media for a multi-media session. This response is sent to the S-CSCF.

6. The S-CSCF forwards the Offer Response message to the P-CSCF.

7. The optional PCC interaction; for example, the PCC filters may be used to prevent unauthorized traffic on the emergency bearer.

8. The P-CSCF forwards the message to the originating endpoint.

9. UE decides the offered set of media streams for this session, confirms receipt of the Offer Response and sends the Response Confirmation to P-CSCF. The Response Confirmation may also contain SDP. This may be the same SDP as in the Offer Response received in Step 8 or a subset. If new media are defined by this SDP, a new authorization (as in Step 7) will be done by the P-CSCF(PDF) following Step 15. The originating UE is free to continue to offer new media on this operation or on subsequent exchanges using the Update method. Each offer/answer exchange will cause the P-CSCF(PDF) to repeat the Authorization step (Step 7) again.

10. UE initiates resource reservation for the offered media.

11. The P-CSCF forwards this message to the S-CSCF.

12. The S-CSCF forwards this message toward the PSAP/emergency center.

13. The PSAP/emergency center responds to the Response Confirmation with an acknowledgement. If Optional SDP is contained in the Response Confirmation, the Confirmation Ack will also contain an SDP response.

14. The PSAP/emergency center initiates the reservation procedures for the resources needed for this session.

15. The S-CSCF forwards the response to the P-CSCF.

16. The P-CSCF forwards the response to UE.

17.-19. When the resource reservation is completed, UE sends the successful Resource Reservation message to the terminating endpoint, via the signalling path established by the INVITE message. The message is sent first to the P-CSCF.

20. The destination user may be alerted of an incoming session setup attempt.

21.-23. The PSAP/emergency center responds to the successful resource reservation and the message is forwarded to the originating end.

24.-26. The PSAP/emergency center may have alerted the user and may be waiting for an indication from the user before completing the session. If so, it indicates this to the originating party by a provisional response indicating Ringing. This message is sent to the S-CSCF and along the signalling path to the originating end.

27. The UE indicates to the originating user that the destination is ringing

28. When the destination party answers, PSAP/emergency center sends a SIP 200-OK final response to the S-CSCF.

29. The PSAP/emergency center starts the media flow(s) for this session.

30. The S-CSCF forwards the 200-OK to the P-CSCF

31. The optional PCC interaction; for example, the PCC filters may be used to prevent unauthorized traffic on the emergency bearer.

32. The P-CSCF sends a SIP 200-OK final response to the session originator.

33. The UE starts the media flow(s) for this session.

34.-36. The UE responds to the 200 OK with a SIP ACK message sent along the signalling path.

5.3.1.2 PSAP/Emergency center located at the GSTN

This procedure applies when an emergency center or PSAP is located in the GSTN (in the PSTN networks or CS domain).

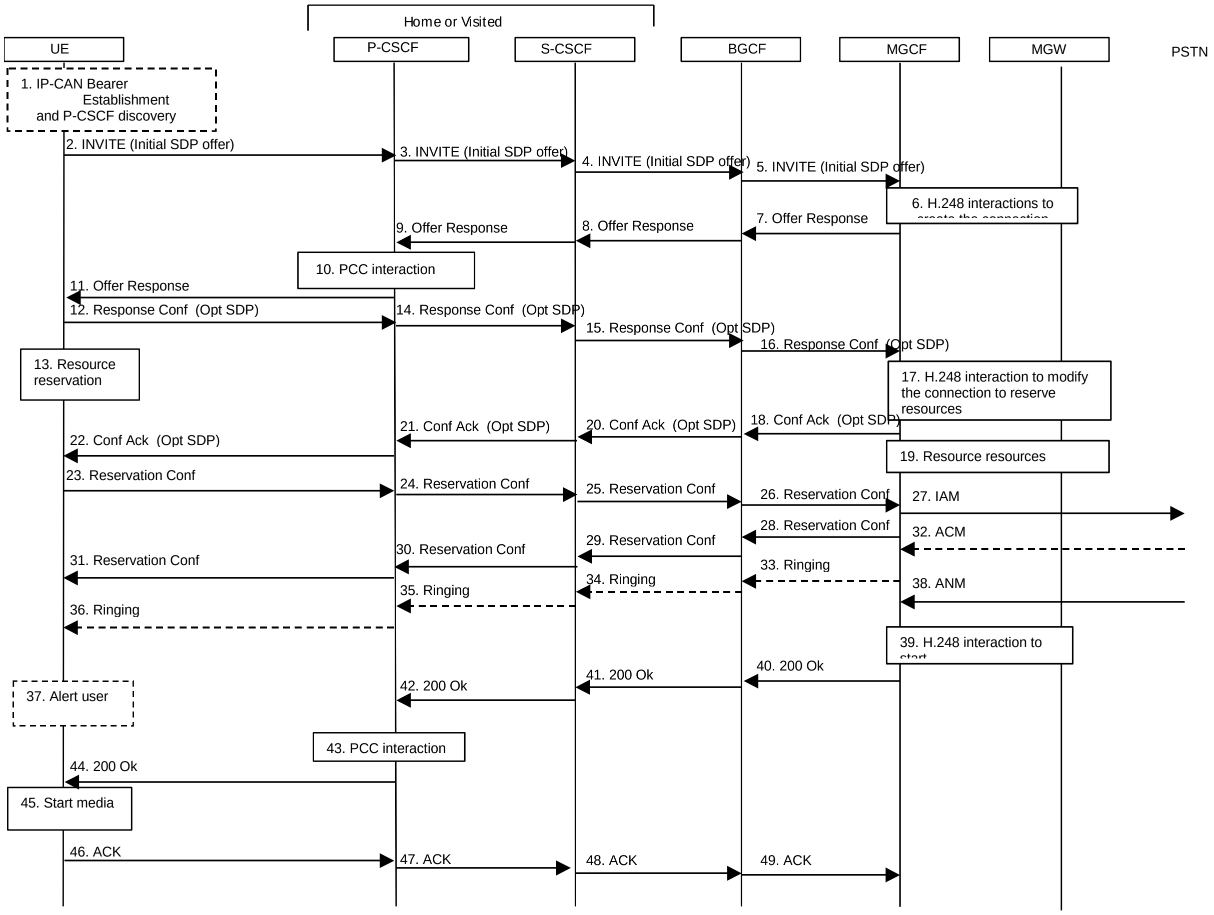

Figure 5.2: Emergency session establishment – PSAP/emergency centre located at the PSTN

1. In order to establish an IMS emergency session the UE must have an IP-CAN Bearer to be used for IMS related signalling and must have discovered a P-CSCF. P-CSCF discovery should use the PDP Context Activation mechanism where the P-CSCF address is sent to the UE in the Activate PDP Context Accept message.

2. UE sends the SIP INVITE request, containing an initial SDP, to the P-CSCF. The initial SDP may represent one or more media for a multi-media session. The SIP INVITE shall contain location information and it shall contain an emergency session indication when the UE has detected the emergency session itself.

3. When the P-CSCF receives an emergency SIP INVITE request it forwards the SIP INVITE request to a pre-configured S-CSCF in the same network. If an emergency indication was not set by the UE, then the P-CSCF returns a 380 (Alternative Service) response with the type set to "emergency".

4. The S-CSCF uses the location of the UE to identify the next hop. The S-CSCF determines that this is for the PSTN, and passes the request to the BGCF. To route the emergency call through the GSTN to the correct PSAP or emergency centre the S-CSCF translates the received SIP-URI or Tel-URL based on the location of the UE and additionally other information such as type of emergency service into a routable number. The S-CSCF may e.g. send this number as a Tel-URL to the BGCF. This number shall have the same format as used for CS emergency calls.

5. The BGCF forwards the request to the MGCF.

6. MGCF receives an INVITE request, containing an initial SDP and it initiates a H.248 interaction to pick an outgoing channel and determine media capabilities of the MGW.

7.-9. MGCF determines the subset of the media flows proposed by the originating endpoint that it supports, and responds with an Offer Response message back to the originator.

10. The optional PCC interaction; for example, the PCC filters may be used to prevent unauthorized traffic on the emergency bearer.

11. The P-CSCF forwards the message to the originating endpoint.

12. UE decides the offered set of media streams for this session, confirms receipt of the Offer Response and sends the Response Confirmation to P-CSCF. The Response Confirmation may also contain SDP. This may be the same SDP as in the Offer Response received in Step 11 or a subset. If new media are defined by this SDP, a new authorization (as in Step 10) will be done by the P-CSCF(PDF) following Step 21. The originating UE is free to continue to offer new media on this operation or on subsequent exchanges using the Update method. Each offer/answer exchange will cause the P-CSCF(PDF) to repeat the Authorization step (Step 10) again.

13. UE initiates resource reservation for the offered media.

14. The P-CSCF forwards this message to the S-CSCF.

15. The S-CSCF forwards this message to the BGCF.

16. The BGCF forwards this message to the MGCF.

17. MGCF initiates a H.248 interaction to modify the connection established in step #6 and instruct MGW to reserve the resources necessary for the media streams.

18.-22. MGCF responds to the offered media towards the originating party.

23.-26. When the resource reservation is completed, UE sends the successful Resource Reservation message to the terminating endpoint, via the signalling path established by the INVITE message. The message is sent first to the P-CSCF.

27. MGCF sends an IAM message to the PSTN.

28.-31. MGCF sends response to the successful resource reservation towards originating end.

32. The PSTN establishes the path to the destination. It may optionally alert the destination user before completing the session. If so, it responds with an ACM message.

33.-36.The PSAP/emergency centre may have alerted the user and may be waiting for an indication from the user before completing the session. If so, it indicates this to the originating party by a provisional response indicating Ringing. This message is sent along the signalling path to the originating end.

37. The UE indicates to the originating user that the destination is ringing.

38. When the destination party answers, the PSTN sends an ANM message to MGCF.

39. MGCF initiates a H.248 interaction to make the connection in the MGW bi-directional.

40.-42. MGCF sends a SIP 200-OK final response along the signalling path back to the session originator.

43. The optional PCC interaction; for example, the PCC filters may be used to prevent unauthorized traffic on the emergency bearer.

44. The P-CSCF sends a SIP 200-OK final response to the session originator.

45. The UE starts the media flow(s) for this session.

46.-49. The UE responds to the 200 OK with a SIP ACK message sent along the signalling path.

6 Impacts on IP-Connectivity Access Network

6.1 General

In order to establish an IMS emergency session the UE needs to have a PDP context to be used for IMS related signalling and optionally a secondary PDP context for the media related to the emergency session.

The network identifies that a PDP context is being activated for emergency use (signalling and media context) when the UE provides the globally dedicated emergency APN in the PDP context activation procedure. This allows the network to apply special treatment (e.g. with respect to filtering, higher priority, routing, QoS) to IMS emergency sessions.

Whenever a UE is knowingly establishing an emergency service session using the PS domain (i.e., it has either recognized the request from the user or received a 380 response to an unrecognised request), it shall attempt to establish a primary PDP context for signalling, indicating that the context is for emergency use, and including a request for a P-CSCF assignment. This will be done even if the UE already has a PDP context for its use. This should allow for optimised establishment of the PDP context and for the IMS signalling path.

If the UE is not attached to GPRS network, then it shall first perform a GPRS attach. It shall be possible for the network to discriminate between a normal Attach and an Attach for emergency use.

The terminal handling for emergency session requests when some terminal resource is unavailable (e.g., all supported PDP contexts active), is for further study.

6.2 General Packet Radio Service (GPRS) for UICC case

6.2.1 GPRS Attach Function

Note: the term 'emergency GPRS Attach' refers to an attach procedure that is initiated for emergency use.

In case of emergency GPRS attach, the MS shall provide an emergency indication to the network. This indication allows the network to apply special treatment for the user during the attach procedure.

Support of an emergency attach is subject to operator's policy and regulatory requirements but it should avoid use of normal roaming restrictions and subscription checking.

The network may also apply certain rules to PDP context activation and deactivation for emergency use after the emergency GPRS attach procedure is completed.

An emergency GPRS attach shall be performed if the UE is not attached to GPRS. The emergency GPRS attach shall not be performed, when the MS is already attached to GPRS.

The Combined GPRS/IMSI Attach procedure is illustrated in Figure 6.1.

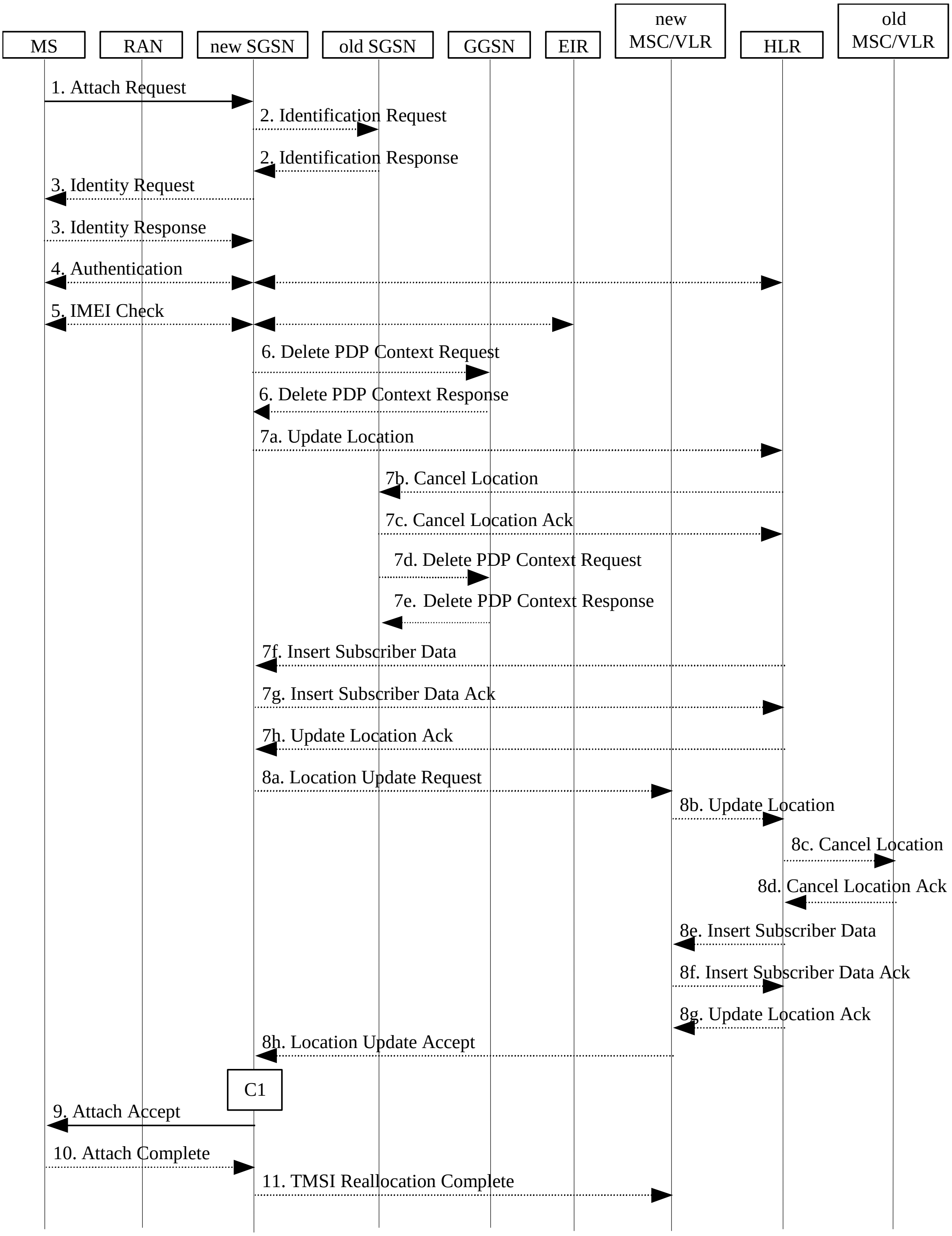
MS
RAN
new SGSN
old SGSN
GGSN
EIR
new MSC/VLR
HLR
old MSC/VLR
1. Attach Request
2. Identification Request
2. Identification Response
3. Identity Request
3. Identity Response
4. Authentication
5. IMEI Check
6. Delete PDP Context Request
6. Delete PDP Context Response
7a. Update Location
7b. Cancel Location
7c. Cancel Location Ack
7d. Delete PDP Context Request
7e. Delete PDP Context Response
7f. Insert Subscriber Data
7g. Insert Subscriber Data Ack
7h. Update Location Ack
8a. Location Update Request
8b. Update Location
8c. Cancel Location
8d. Cancel Location Ack
8e. Insert Subscriber Data
8f. Insert Subscriber Data Ack
8g. Update Location Ack
8h. Location Update Accept
C1
9. Attach Accept
10. Attach Complete
11. TMSI Reallocation Complete

Figure 6.1: Combined GPRS/IMSI Attach Procedure

1) In A/Gb mode, the MS initiates the attach procedure by the transmission of an Attach Request (IMSI or P-TMSI and old RAI, Classmark, CKSN, Attach Type, DRX Parameters, old P-TMSI Signature, Emergency Indication) message to the SGSN. IMSI shall be included if the MS does not have a valid P-TMSI available. If the MS has a valid P-TMSI, then P-TMSI and the old RAI associated with P-TMSI shall be included. Classmark contains the MS's GPRS multislot capabilities and supported GPRS ciphering algorithms in addition to the existing classmark parameters defined in GSM 04.08. Attach Type indicates which type of attach is to be performed, i.e. GPRS attach only, GPRS Attach while already IMSI attached, or combined GPRS / IMSI attach. DRX Parameters indicates whether the MS uses discontinuous reception or not. If the MS uses discontinuous reception, then DRX Parameters also indicate when the MS is in a non-sleep mode able to receive paging requests and channel assignments. If the MS uses P-TMSI for identifying itself and if it has also stored its old P-TMSI Signature, then the MS shall include the old P-TMSI Signature in the Attach Request message.

   For Iu mode, the MS initiates the attach procedure by the transmission of an Attach Request (IMSI or P-TMSI and old RAI, Core Network Classmark, KSI, Attach Type, old P-TMSI Signature, Follow On Request, DRX Parameters, Emergency Indication) message to the SGSN. IMSI shall be included if the MS does not have a valid P-TMSI available. If the MS uses P-TMSI for identifying itself and if it has also stored its old P-TMSI Signature, then the MS shall include the old P-TMSI Signature in the Attach Request message. If the MS has a valid P-TMSI, then P-TMSI and the old RAI associated with P-TMSI shall be included. KSI shall be included if the MS has valid security parameters. Core Network Classmark is described in clause "MS Network Capability". The MS shall set "Follow On Request Pending" if there is pending uplink traffic (signalling or user data). MS shall set Follow On Request to "Follow On Request Pending" in case attach is requested for emergency use. The SGSN may use, as an implementation option, the follow on request indication to release or keep the Iu connection after the completion of the GPRS Attach procedure. In case MS is requesting attach for emergency use, the SGSN shall keep the Iu connection for not delaying emergency call setup. Attach Type indicates which type of attach is to be performed, i.e. GPRS attach only, GPRS Attach while already IMSI attached, or combined GPRS / IMSI attach. DRX Parameters indicates whether or not the MS uses discontinuous reception and the DRX cycle length.

   When the Attach is requested for emergency use, the MS shall include an Emergency Indication in the Attach Request.

2) If the MS identifies itself with P-TMSI and the SGSN has changed since detach, the new SGSN sends an Identification Request (P-TMSI, old RAI, old P-TMSI Signature) to the old SGSN to request the IMSI. If the new SGSN provides functionality for Intra Domain Connection of RAN Nodes to Multiple CN Nodes, the new SGSN may derive the old SGSN from the old RAI and the old P-TMSI and send the Identification Request message to this old SGSN. Otherwise, the new SGSN derives the old SGSN from the old RAI. In any case the new SGSN will derive an SGSN that it believes is the old SGSN. This derived SGSN is itself the old SGSN, or it is associated with the same pool area as the actual old SGSN and it will determine the correct old SGSN from the P-TMSI and relay the message to that actual old SGSN. The old SGSN responds with Identification Response (IMSI, Authentication Triplets or Authentication Quintets). If the MS is not known in the old SGSN, the old SGSN responds with an appropriate error cause. The old SGSN also validates the old P-TMSI Signature and responds with an appropriate error cause if it does not match the value stored in the old SGSN.

3) If the MS is unknown in both the old and new SGSN, the SGSN sends an Identity Request (Identity Type = IMSI) to the MS. The MS responds with Identity Response (IMSI).

4) The authentication functions are defined in the clause "Security Function". If no MM context for the MS exists anywhere in the network, then authentication is mandatory. Ciphering procedures are described in clause "Security Function". If P-TMSI allocation is going to be done and the network supports ciphering, the network shall set the ciphering mode.

5) The equipment checking functions are defined in the clause "Identity Check Procedures". Equipment checking is optional.

6) If there are active PDP contexts in the new SGSN for this particular MS (i.e. the MS re-attaches to the same SGSN without having properly detached before), the new SGSN deletes these PDP contexts by sending Delete PDP Context Request (TEID) messages to the GGSNs involved. The GGSNs acknowledge with Delete PDP Context Response (TEID) messages.

7) If the SGSN number has changed since the GPRS detach, or if it is the very first attach, then the SGSN informs the HLR:

   a) The SGSN sends an Update Location (SGSN Number, SGSN Address, IMSI) to the HLR.

b) The HLR sends Cancel Location (IMSI, Cancellation Type) to the old SGSN with Cancellation Type set to Update Procedure.

c) The old SGSN acknowledges with Cancel Location Ack (IMSI). If there are any ongoing procedures for that MS, the old SGSN shall wait until these procedures are finished before removing the MM and PDP contexts.

d) If there are active PDP contexts in the old SGSN for this particular MS, the old SGSN deletes these PDP contexts by sending Delete PDP Context Request (TEID) messages to the GGSNs involved.

e) The GGSNs acknowledge with Delete PDP Context Response (TEID) messages.

f) The HLR sends Insert Subscriber Data (IMSI, GPRS Subscription Data) to the new SGSN.

g) The new SGSN validates the MS's presence in the (new) RA. If due to regional subscription restrictions the MS is not allowed to attach in the RA, the SGSN rejects the Attach Request with an appropriate cause, and may return an Insert Subscriber Data Ack (IMSI, SGSN Area Restricted) message to the HLR. If subscription checking fails for other reasons, the SGSN rejects the Attach Request with an appropriate cause and returns an Insert Subscriber Data Ack (IMSI, Cause) message to the HLR. If the MS is making Attach for emergency use, the SGSN should not reject the Attach due to e.g. roaming restrictions. If all checks are successful then the SGSN constructs an MM context for the MS and returns an Insert Subscriber Data Ack (IMSI) message to the HLR.

h) The HLR acknowledges the Update Location message by sending an Update Location Ack to the SGSN after the cancelling of old MM context and insertion of new MM context are finished. If the Update Location is rejected by the HLR, the SGSN rejects the Attach Request from the MS with an appropriate cause.

8) If Attach Type in step 1 indicated GPRS Attach while already IMSI attached, or combined GPRS / IMSI attached, then the VLR shall be updated if the Gs interface is installed. When the SGSN does not provide functionality for the Intra Domain Connection of RAN Nodes to Multiple CN Nodes, the VLR number is derived from the RAI. When the SGSN provides functionality for Intra Domain Connection of RAN Nodes to Multiple CN Nodes, the SGSN uses the RAI and a hash value from the IMSI to determine the VLR number. The SGSN starts the location update procedure towards the new MSC/VLR upon receipt of the first Insert Subscriber Data message from the HLR in step 6d). This operation marks the MS as GPRS-attached in the VLR.

a) The SGSN sends a Location Update Request (new LAI, IMSI, SGSN Number, Location Update Type) message to the VLR. Location Update Type shall indicate IMSI attach if Attach Type indicated combined GPRS/IMSI attach. Otherwise, Location Update Type shall indicate normal location update. The VLR creates an association with the SGSN by storing SGSN Number.

b) If the LA update is inter-MSC, the new VLR sends Update Location (IMSI, new VLR) to the HLR.

c) If the LA update is inter-MSC, the HLR sends a Cancel Location (IMSI) to the old VLR.

d) The old VLR acknowledges with Cancel Location Ack (IMSI).

e) If the LA update is inter-MSC, the HLR sends Insert Subscriber Data (IMSI, subscriber data) to the new VLR.

f) The VLR acknowledges with Insert Subscriber Data Ack (IMSI).

g) After finishing the inter-MSC location update procedures, the HLR responds with Update Location Ack (IMSI) to the new VLR.

h) The VLR responds with Location Update Accept (VLR TMSI) to the SGSN.

9) The SGSN selects Radio Priority SMS, and sends an Attach Accept (P-TMSI, VLR TMSI, P-TMSI Signature, Radio Priority SMS) message to the MS. P-TMSI is included if the SGSN allocates a new P-TMSI.

10) If P-TMSI or VLR TMSI was changed, the MS acknowledges the received TMSI(s) by returning an Attach Complete message to the SGSN.

11) If VLR TMSI was changed, the SGSN confirms the VLR TMSI re-allocation by sending a TMSI Reallocation Complete message to the VLR.

If the Attach Request cannot be accepted, the SGSN returns an Attach Reject (IMSI, Cause) message to the MS.

The CAMEL procedure call shall be performed, see referenced procedure in TS 23.078:

C1) CAMEL_GPRS_Attach and CAMEL_PS_Notification.

They are called in the following order:

- The procedure CAMEL_GPRS_Attach is called. In figure 6.1, the procedure returns as result "Continue".

Then the procedure CAMEL_PS_Notification is called. The procedure returns as result "Continue".

6.2.2 GPRS Detach Function

It is a network option whether to detach the MS for emergency use after the emergency PDP contexts have been deactivated (i.e. once the emergency use is finished). If the MS is detached after emergency use, an appropiate cause shall be sent to the MS.

6.2.3 Location Management Function

6.2.3.1 Routeing Area Update Procedure

6.2.3.1.1 Intra SGSN Routeing Area Update

The Intra SGSN Routeing Area Update procedure is illustrated in figure 6.2.

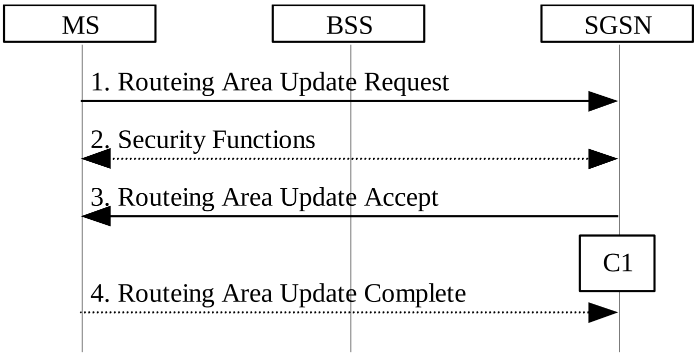
MS
BSS
SGSN
1. Routeing Area Update Request
2. Security Functions
3. Routeing Area Update Accept
C1
4. Routeing Area Update Complete

Figure 6.2: Intra SGSN Routeing Area Update Procedure

1) The MS sends a Routeing Area Update Request (P-TMSI, old RAI, old P-TMSI Signature, Update Type) to the SGSN. Update Type shall indicate RA update or periodic RA update. The BSS shall add the Cell Global Identity including the RAC and LAC of the cell where the message was received before passing the message to the SGSN, see GSM 08.18 [21].

2) Security functions may be executed. These procedures are defined in subclause "Security Function".

3) The SGSN validates the MS's presence in the new RA. If, due to regional subscription restrictions, the MS is not allowed to be attached in the RA, or if subscription checking fails, the SGSN rejects the routeing area update with an appropriate cause. If the MS is emergency attached or if the MS has active PDP context(s) for an emergency use, the SGSN should not reject the routing area update due to e.g. roaming restrictions. If all checks are successful, the SGSN updates the MM context for the MS. A new P-TMSI may be allocated. A Routeing Area Update Accept (P-TMSI, P-TMSI Signature) is returned to the MS.

4) If P-TMSI was reallocated, the MS acknowledges the new P-TMSI by returning a Routeing Area Update Complete message to the SGSN.

If the routeing area update procedure fails a maximum allowable number of times, or if the SGSN returns a Routeing Area Update Reject (Cause) message, the MS shall enter IDLE state.

The CAMEL procedure calls shall be performed, see referenced procedure in TS 23.078, C1:

C1) CAMEL_GPRS_Routeing_Area_Update_Session, CAMEL_PS_Notification and CAMEL_GPRS_Routeing_Area_Update_Context.

They are called in the following order:

- The procedure CAMEL_GPRS_Routeing_Area_Update_Session is called once per session. It returns as a result "Continue".
- Then the procedure CAMEL_PS_Notification is called once per session. It returns as a result "Continue".
- Then the procedure CAMEL_GPRS_Routeing_Area_Update_Context is called once per PDP context. It returns as a result "Continue".

6.2.3.1.2 Inter SGSN Routeing Area Update

The Inter SGSN Routeing Area Update procedure is illustrated in figure 6.3.

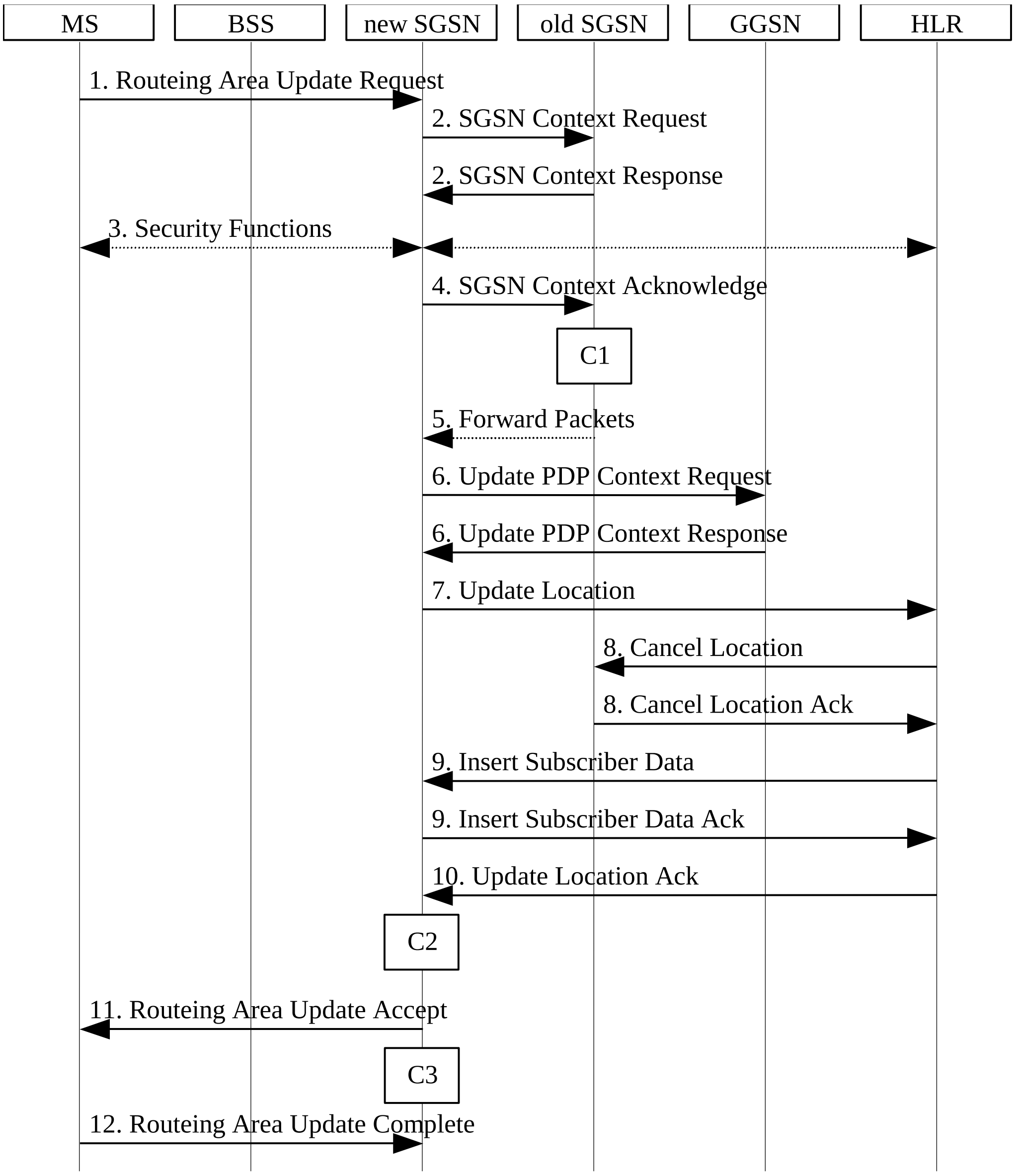
MS
BSS
new SGSN
old SGSN
GGSN
HLR
1. Routeing Area Update Request
2. SGSN Context Request
2. SGSN Context Response
3. Security Functions
4. SGSN Context Acknowledge
C1
5. Forward Packets
6. Update PDP Context Request
6. Update PDP Context Response
7. Update Location
8. Cancel Location
8. Cancel Location Ack
9. Insert Subscriber Data
9. Insert Subscriber Data Ack
10. Update Location Ack
C2
11. Routeing Area Update Accept
C3
12. Routeing Area Update Complete

Figure 6.3: Inter SGSN Routeing Area Update Procedure

1) The MS sends a Routeing Area Update Request (old RAI, old P-TMSI Signature, Update Type, Classmark, DRX parameters and MS Network Capability) to the new SGSN. Update Type shall indicate RA update or periodic RA update. The BSS shall add the Cell Global Identity including the RAC and LAC of the cell where the message was received before passing the message to the SGSN. Classmark contains the MS GPRS multislot capabilities and supported GPRS ciphering algorithms as defined in TS 24.008. DRX Parameters indicates whether or not the MS uses discontinuous reception and the DRX cycle length.

2) The new SGSN sends SGSN Context Request (old RAI, TLLI, old P-TMSI Signature, New SGSN Address) to the old SGSN to get the MM and PDP contexts for the MS. If the new SGSN provides functionality for Intra Domain Connection of RAN Nodes to Multiple CN Nodes, the new SGSN may derive the old SGSN from the old RAI and the old P-TMSI (or TLLI) and send the SGSN Context Request message to this old SGSN. Otherwise, the new SGSN derives the old SGSN from the old RAI. In any case the new SGSN will derive an SGSN that it believes is the old SGSN. This derived SGSN is itself the old SGSN, or it is associated with the same pool area as the actual old SGSN and it will determine the correct old SGSN from the P-TMSI (or TLLI) and relay the message to that actual old SGSN. The old SGSN validates the old P-TMSI Signature and responds with an appropriate error cause if it does not match the value stored in the old SGSN. This should initiate the security functions in the new SGSN. If the security functions authenticate the MS correctly, the new SGSN shall send an SGSN Context Request (old RAI, TLLI, MS Validated, New SGSN Address) message to the old SGSN. MS Validated indicates that the new SGSN has authenticated the MS. If the old P-TMSI Signature was valid or if the new SGSN indicates that it has authenticated the MS, the old SGSN stops assigning SNDCP N-PDU numbers to downlink N-PDUs received, and responds with SGSN Context Response (MM Context, PDP Contexts). If the MS is not known in the old SGSN, the old SGSN responds with an appropriate error cause. The old SGSN stores New SGSN Address, to allow the old SGSN to forward data packets to the new SGSN. Each PDP Context includes the SNDCP Send N-PDU Number for the next downlink N-PDU to be sent in acknowledged mode to the MS, the SNDCP Receive N-PDU Number for the next uplink N-PDU to be received in acknowledged mode from the MS, the GTP sequence number for the next downlink N-PDU to be sent to the MS and the GTP sequence number for the next uplink N-PDU to be tunnelled to the GGSN. The old SGSN starts a timer and stops the transmission of N-PDUs to the MS. The new SGSN shall ignore the MS Network Capability contained in MM Context of SGSN Context Response only when it has previously received an MS Network Capability in the Routeing Area Request.

3) Security functions may be executed. These procedures are defined in clause "Security Function". Ciphering mode shall be set if ciphering is supported.

   If the security functions fail (e.g. because the SGSN cannot determine the HLR address to establish the Send Authentication Info dialogue), the Inter SGSN RAU Update procedure fails. A reject shall be returned to the MS with an appropriate cause.

   If the MS is emergency attached or if the MS has active PDP contexts for an emergency use, security functions may be executed (serving network option).

4) The new SGSN sends an SGSN Context Acknowledge message to the old SGSN. This informs the old SGSN that the new SGSN is ready to receive data packets belonging to the activated PDP contexts. The old SGSN marks in its context that the MSC/VLR association and the information in the GGSNs and the HLR are invalid. This triggers the MSC/VLR, the GGSNs, and the HLR to be updated if the MS initiates a routeing area update procedure back to the old SGSN before completing the ongoing routeing area update procedure. If the security functions do not authenticate the MS correctly, then the routeing area update shall be rejected, and the new SGSN shall send a reject indication to the old SGSN. The old SGSN shall continue as if the SGSN Context Request was never received.

5) The old SGSN duplicates the buffered N-PDUs and starts tunnelling them to the new SGSN. Additional N-PDUs received from the GGSN before the timer described in step 2 expires are also duplicated and tunnelled to the new SGSN. N-PDUs that were already sent to the MS in acknowledged mode and that are not yet acknowledged by the MS are tunnelled together with the SNDCP N-PDU number. No N-PDUs shall be forwarded to the new SGSN after expiry of the timer described in step 2.

6) The new SGSN sends Update PDP Context Request (new SGSN Address, TEID, QoS Negotiated) to the GGSNs concerned. The GGSNs update their PDP context fields and return Update PDP Context Response (TEID).

7) The new SGSN informs the HLR of the change of SGSN by sending Update Location (SGSN Number, SGSN Address, IMSI) to the HLR.

8) The HLR sends Cancel Location (IMSI, Cancellation Type) to the old SGSN with Cancellation Type set to Update Procedure. If the timer described in step 2 is not running, the old SGSN removes the MM and PDP contexts. Otherwise, the contexts are removed only when the timer expires. This allows the old SGSN to complete the forwarding of N-PDUs. It also ensures that the MM and PDP contexts are kept in the old SGSN in case the MS initiates another inter-SGSN routeing area update before completing the ongoing routeing area update to the new SGSN. The old SGSN acknowledges with Cancel Location Ack (IMSI).

9) The HLR sends Insert Subscriber Data (IMSI, GPRS Subscription Data) to the new SGSN. The new SGSN validates the MS's presence in the (new) RA. If due to regional subscription restrictions the MS is not allowed to be attached in the RA, the SGSN rejects the Routeing Area Update Request with an appropriate cause, and may return an Insert Subscriber Data Ack (IMSI, SGSN Area Restricted) message to the HLR. If all checks are successful, the SGSN constructs an MM context for the MS and returns an Insert Subscriber Data Ack (IMSI) message to the HLR.

10) The HLR acknowledges the Update Location by sending Update Location Ack (IMSI) to the new SGSN.

11) The new SGSN validates the MS's presence in the new RA. If due to roaming restrictions the MS, is not allowed to be attached in the SGSN, or if subscription checking fails, the new SGSN rejects the routeing area update with an appropriate cause. If the MS is emergency attached or if the MS has active PDP context(s) for an emergency use, the SGSN should not reject the routing area update due to e.g. roaming restrictions. If all checks are successful, the new SGSN constructs MM and PDP contexts for the MS. A logical link is established between the new SGSN and the MS. The new SGSN responds to the MS with Routeing Area Update Accept (P-TMSI, P-TMSI Signature, Receive N-PDU Number). Receive N-PDU Number contains the acknowledgements for each acknowledged-mode NSAPI used by the MS, thereby confirming all mobile-originated N-PDUs successfully transferred before the start of the update procedure.

12) The MS acknowledges the new P-TMSI by returning a Routeing Area Update Complete (Receive N-PDU Number) message to the SGSN. Receive N-PDU Number contains the acknowledgements for each acknowledged-mode NSAPI used by the MS, thereby confirming all mobile-terminated N-PDUs successfully transferred before the start of the update procedure. If Receive N-PDU Number confirms reception of N-PDUs that were forwarded from the old SGSN, these N-PDUs shall be discarded by the new SGSN. LLC and SNDCP in the MS are reset.

In the case of a rejected routeing area update operation, due to regional subscription or roaming restrictions, or because the SGSN cannot determine the HLR address to establish the locating updating dialogue, the new SGSN shall not construct an MM context. A reject shall be returned to the MS with an appropriate cause. The MS does not re-attempt a routeing area update to that RA. The RAI value shall be deleted when the MS is powered-up.

If the new SGSN is unable to update the PDP context in one or more GGSNs, the new SGSN shall deactivate the corresponding PDP contexts as described in clause "SGSN-initiated PDP Context Deactivation Procedure". This shall not cause the SGSN to reject the routeing area update.

The PDP Contexts shall be sent from old to new SGSN in a prioritized order, i.e. the most important PDP Context first in the SGSN Context Response message. (The prioritization method is implementation dependent, but should be based on the current activity.)

If the new SGSN is unable to support the same number of active PDP contexts as received from old SGSN, the new SGSN should use the prioritisation sent by old SGSN as input when deciding which PDP contexts to maintain active and which ones to delete. PDP contexts related to an emergency use shall have a high priority and therefore PDP contexts for emergency use should not be deactivated during the routeing area update. In any case, the new SGSN shall first update all contexts in one or more GGSNs and then deactivate the context(s) that it cannot maintain as described in subclause "SGSN-initiated PDP Context Deactivation Procedure". This shall not cause the SGSN to reject the routeing area update.

If the timer described in step 2 expires and no Cancel Location (IMSI) was received from the HLR, the old SGSN stops forwarding N-PDUs to the new SGSN.

If the routeing area update procedure fails a maximum allowable number of times, or if the SGSN returns a Routeing Area Update Reject (Cause) message, the MS shall enter IDLE state.

The CAMEL procedure calls shall be performed, see referenced procedures in TS 23.078:

C1) CAMEL_GPRS_PDP_Context_Disconnection, CAMEL_GPRS_Detach and CAMEL_PS_Notification.

They are called in the following order:

- The CAMEL_GPRS_PDP_Context_Disconnection procedure is called several times: once per PDP context. The procedure returns as result "Continue".
- Then the CAMEL_GPRS_Detach procedure is called once. The procedure returns as result "Continue".
- Then the CAMEL_PS_Notification procedure is called once. The procedure return as result "Continue".

C2) CAMEL_GPRS_Routeing_Area_Update_Session and CAMEL_PS_Notification.

They are called in the following order:

- The CAMEL_GPRS_Routeing_Area_Update_Session procedure is called. The procedure returns as result "Continue".
- Then the CAMEL_PS_Notification procedure is called. The procedure returns as result "Continue".

C3) CAMEL_GPRS_Routeing_Area_Update_Context.

This procedure is called several times: once per PDP context. It returns as result "Continue".

6.2.3.2 Combined RA/LA Update Procedure

A combined RA/LA update takes place in network operation mode I when the MS enters a new RA or when a GPRS-attached MS performs an IMSI attach or when the MS has to indicate new access capabilities to the network, or when a suspended MS is not resumed by the BSS (see subclause "Suspension of GPRS Services"). The MS sends a Routeing Area Update Request indicating that an LA update may also need to be performed, in which case the SGSN forwards the LA update to the VLR. This concerns only idle mode (see GSM 03.22), as no combined RA/LA updates are performed during a CS connection.

6.2.3.2.1 Combined Intra SGSN RA/LA Update

The Combined RA/LA Update (intra SGSN) procedure is illustrated in Figure 6.4.

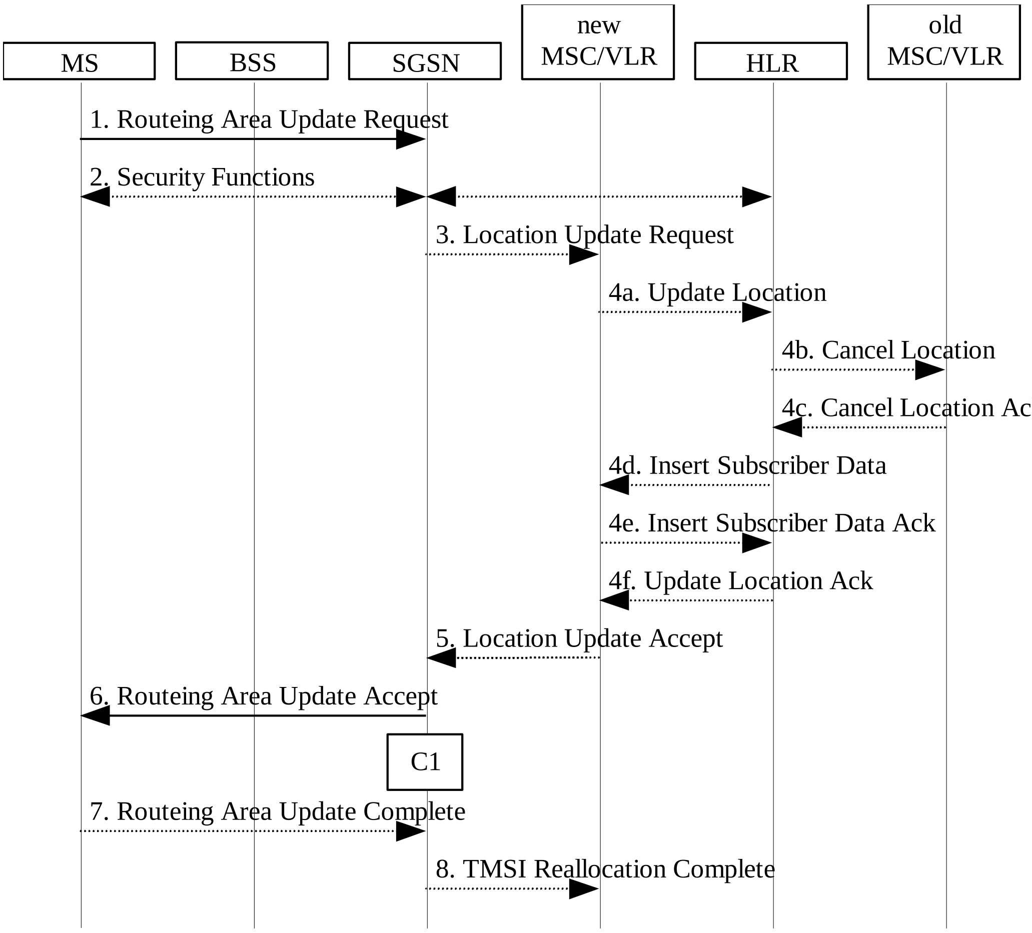
MS
BSS
SGSN
new MSC/VLR
HLR
old MSC/VLR
1. Routeing Area Update Request
2. Security Functions
3. Location Update Request
4a. Update Location
4b. Cancel Location
4c. Cancel Location Ack
4d. Insert Subscriber Data
4e. Insert Subscriber Data Ack
4f. Update Location Ack
5. Location Update Accept
6. Routeing Area Update Accept
C1
7. Routeing Area Update Complete
8. TMSI Reallocation Complete

Figure 6.4: Combined RA/LA Update in the Case of Intra SGSN RA Update Procedure

1) The MS sends a Routeing Area Update Request (old RAI, old P-TMSI Signature, Update Type) to the SGSN. Update Type shall indicate combined RA/LA update, or, if the MS wants to perform an IMSI attach, combined

RA/LA update with IMSI attach requested. The BSS shall add the Cell Global Identity including the RAC and LAC of the cell where the message was received before passing the message to the SGSN.

2) Security functions may be executed. This procedure is defined in clause "Security Function". If the security functions fail (e.g. because the SGSN cannot determine the HLR address to establish the Send Authentication Info dialogue), the Inter SGSN RAU Update procedure fails. A reject shall be returned to the MS with an appropriate cause.

3) If the association has to be established, if Update Type indicates combined RA/LA update with IMSI attach requested, or if the LA changed with the routeing area update, the SGSN sends a Location Update Request (new LAI, IMSI, SGSN Number, Location Update Type) to the VLR. Location Update Type shall indicate IMSI attach if Update Type in step 1 indicated combined RA/LA update with IMSI attach requested. Otherwise, Location Update Type shall indicate normal location update. When the SGSN does not provide functionality for the Intra Domain Connection of RAN Nodes to Multiple CN Nodes, the VLR number is derived from the RAI. When the SGSN provides functionality for Intra Domain Connection of RAN Nodes to Multiple CN Nodes, the SGSN uses the RAI and a hash value from the IMSI to determine the VLR number. The VLR creates or updates the association with the SGSN by storing SGSN Number.

4) If the subscriber data in the VLR is marked as not confirmed by the HLR, the new VLR informs the HLR. The HLR cancels the data in the old VLR and inserts subscriber data in the new VLR:

   a) The new VLR sends an Update Location (new VLR) to the HLR.

   b) The HLR cancels the data in the old VLR by sending Cancel Location (IMSI) to the old VLR.

   c) The old VLR acknowledges with Cancel Location Ack (IMSI).

   d) The HLR sends Insert Subscriber Data (IMSI, subscriber data) to the new VLR.

   e) The new VLR acknowledges with Insert Subscriber Data Ack (IMSI).

   f) The HLR responds with Update Location Ack (IMSI) to the new VLR.

5) The new VLR allocates a new VLR TMSI and responds with Location Update Accept (VLR TMSI) to the SGSN. VLR TMSI is optional if the VLR has not changed.

6) The SGSN validates the MS's presence in the new RA. If due to regional subscription restrictions the MS is not allowed to be attached in the RA, or if subscription checking fails, the SGSN rejects the routeing area update with an appropriate cause. If the MS is emergency attached or if the MS has active PDP context(s) for emergency use, the SGSN should not reject the routing area update due to e.g. roaming restrictions. If all checks are successful, the SGSN updates the MM context for the MS. A new P-TMSI may be allocated. The SGSN responds to the MS with Routeing Area Update Accept (P-TMSI, VLR TMSI, P-TMSI Signature).

7) If a new P-TMSI or VLR TMSI was received, the MS confirms the reallocation of the TMSIs by returning a Routeing Area Update Complete message to the SGSN.

8) The SGSN sends a TMSI Reallocation Complete message to the VLR if the MS confirms the VLR TMSI

If the routeing area update procedure fails a maximum allowable number of times, or if the SGSN returns a Routeing Area Update Reject (Cause) message, the MS shall enter IDLE state.

If the Location Update Accept message indicates a reject, this should be indicated to the MS, and the MS shall not access non-GPRS services until a successful Location Update is performed.

The CAMEL procedure calls shall be performed, see referenced procedures in TS 23.078:

C1) CAMEL_GPRS_Routeing_Area_Update_Session, CAMEL_PS_Notification and CAMEL_GPRS_Routeing_Area_Update_Context.

They are called in the following order:

- The procedure CAMEL_GPRS_Routeing_Area_Update_Session is called once per session. In Figure 6.4, the procedure returns as result "Continue".
- Then the procedure CAMEL_PS_Notification is called. The procedure returns as result "Continue".

- Then the procedure CAMEL_GPRS_Routeing_Area_Update_Context is called once per PDP context. In Figure 6.4, the procedure returns as result "Continue".

6.2.3.2.2 Combined Inter SGSN RA/LA Update

The Combined RA/LA Update (inter-SGSN) procedure is illustrated in Figure 6.5.

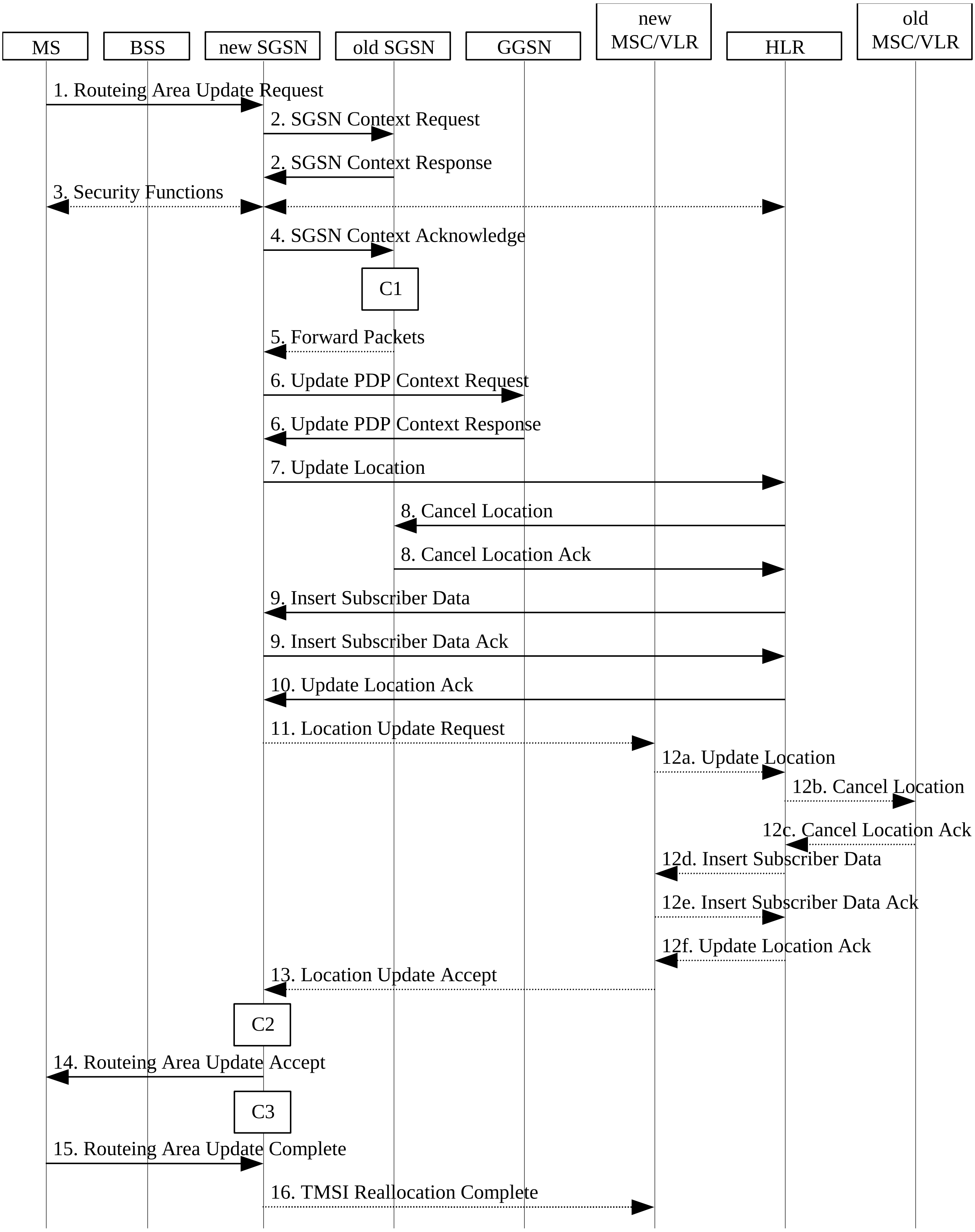
MS
BSS
new SGSN
old SGSN
GGSN
new MSC/VLR
HLR
old MSC/VLR
1. Routeing Area Update Request
2. SGSN Context Request
2. SGSN Context Response
3. Security Functions
4. SGSN Context Acknowledge
C1
5. Forward Packets
6. Update PDP Context Request
6. Update PDP Context Response
7. Update Location
8. Cancel Location
8. Cancel Location Ack
9. Insert Subscriber Data
9. Insert Subscriber Data Ack
10. Update Location Ack
11. Location Update Request
12a. Update Location
12b. Cancel Location
12c. Cancel Location Ack
12d. Insert Subscriber Data
12e. Insert Subscriber Data Ack
12f. Update Location Ack
13. Location Update Accept
C2
14. Routeing Area Update Accept
C3
15. Routeing Area Update Complete
16. TMSI Reallocation Complete

Figure 6.5: Combined RA/LA Update in the Case of Inter SGSN RA Update Procedure

1) The MS sends a Routeing Area Update Request (old RAI, old P-TMSI Signature, Update Type, Classmark, DRX parameters and MS Network Capability) to the new SGSN. Update Type shall indicate combined RA/LA update, or, if the MS wants to perform an IMSI attach, combined RA/LA update with IMSI attach requested. The BSS shall add the Cell Global Identity including the RAC and LAC of the cell where the message was received before passing the message to the SGSN. Classmark contains the MS GPRS multislot capabilities and supported GPRS ciphering algorithms as defined in TS 24.008. DRX Parameters indicates whether or not the MS uses discontinuous and the DRX cycle length.

2) The new SGSN sends SGSN Context Request (old RAI, TLLI, old P-TMSI Signature, New SGSN Address) to the old SGSN to get the MM and PDP contexts for the MS. If the new SGSN provides functionality for Intra Domain Connection of RAN Nodes to Multiple CN Nodes, the new SGSN may derive the old SGSN from the old RAI and the old P-TMSI (or TLLI) and send the SGSN Context Request message to this old SGSN. Otherwise, the new SGSN derives the old SGSN from the old RAI. In any case the new SGSN will derive an SGSN that it believes is the old SGSN. This derived SGSN is itself the old SGSN, or it is associated with the same pool area as the actual old SGSN and it will determine the correct old SGSN from the P-TMSI (or TLLI) and relay the message to that actual old SGSN. The old SGSN validates the old P-TMSI Signature and responds with an appropriate error cause if it does not match the value stored in the old SGSN. This should initiate the security functions in the new SGSN. If the security functions authenticate the MS correctly, the new SGSN shall send an SGSN Context Request (old RAI, TLLI, MS Validated, New SGSN Address) message to the old SGSN. MS Validated indicates that the new SGSN has authenticated the MS. If the old P-TMSI Signature was valid or if the new SGSN indicates that it has authenticated the MS, the old SGSN stops assigning SNDCP N-PDU numbers to downlink N-PDUs received, and responds with SGSN Context Response (MM Context, PDP Contexts). If the MS is not known in the old SGSN, the old SGSN responds with an appropriate error cause. The old SGSN stores New SGSN Address until the old MM context is cancelled, to allow the old SGSN to forward data packets to the new SGSN. Each PDP Context includes the SNDCP Send N-PDU Number for the next downlink N-PDU to be sent in acknowledged mode to the MS, the SNDCP Receive N-PDU Number for the next uplink N-PDU to be received in acknowledged mode from the MS, the GTP sequence number for the next downlink N-PDU to be sent to the MS and the GTP sequence number for the next uplink N-PDU to be tunnelled to the GGSN. The old SGSN starts a timer and stops the downlink transfer. The new SGSN shall ignore the MS Network Capability contained in MM Context of SGSN Context Response only when it has previously received an MS Network Capability in the Routeing Area Request.

3) Security functions may be executed. These procedures are defined in clause "Security Function". Ciphering mode shall be set if ciphering is supported. If the security functions fail (e.g. because the SGSN cannot determine the HLR address to establish the Send Authentication Info dialogue), the Inter SGSN RAU Update procedure fails. A reject shall be returned to the MS with an appropriate cause.

4) The new SGSN sends an SGSN Context Acknowledge message to the old SGSN. This informs the old SGSN that the new SGSN is ready to receive data packets belonging to the activated PDP contexts. The old SGSN marks in its context that the MSC/VLR association and the information in the GGSNs and the HLR are invalid. This triggers the MSC/VLR, the GGSNs, and the HLR to be updated if the MS initiates a routeing area update procedure back to the old SGSN before completing the ongoing routeing area update procedure. If the security functions do not authenticate the MS correctly, the routeing area update shall be rejected, and the new SGSN shall send a reject indication to the old SGSN. The old SGSN shall continue as if the SGSN Context Request was never received.

5) The old SGSN duplicates the buffered N-PDUs and starts tunnelling them to the new SGSN. Additional N-PDUs received from the GGSN before the timer described in step 2 expires are also duplicated and tunnelled to the new SGSN. N-PDUs that were already sent to the MS in acknowledged mode and that are not yet acknowledged by the MS are tunnelled together with the SNDCP N-PDU number. No N-PDUs shall be forwarded to the new SGSN after expiry of the timer described in step 2.

6) The new SGSN sends Update PDP Context Request (new SGSN Address, TEID, QoS Negotiated) to the GGSNs concerned. The GGSNs update their PDP context fields and return an Update PDP Context Response (TEID).

7) The new SGSN informs the HLR of the change of SGSN by sending Update Location (SGSN Number, SGSN Address, IMSI) to the HLR.

8) The HLR sends Cancel Location (IMSI, Cancellation Type) to the old SGSN with Cancellation Type set to Update Procedure. If the timer described in step 2 is not running, the old SGSN removes the MM and PDP contexts. Otherwise, the contexts are removed only when the timer expires. This allows the old SGSN to complete the forwarding of N-PDUs. It also ensures that the MM and PDP contexts are kept in the old SGSN in

case the MS initiates another inter SGSN routeing area update before completing the ongoing routeing area update to the new SGSN. The old SGSN acknowledges with Cancel Location Ack (IMSI).

9) The HLR sends Insert Subscriber Data (IMSI, GPRS Subscription Data) to the new SGSN. The new SGSN validates the MS's presence in the (new) RA. If due to regional subscription restrictions the MS is not allowed to be attached in the RA, the SGSN rejects the Routeing Area Update Request with an appropriate cause, and may return an Insert Subscriber Data Ack (IMSI, SGSN Area Restricted) message to the HLR. If all checks are successful, the SGSN constructs an MM context for the MS and returns an Insert Subscriber Data Ack (IMSI) message to the HLR.

10) The HLR acknowledges the Update Location by sending Update Location Ack (IMSI) to the new SGSN.

11) If the association has to be established, if Update Type indicates combined RA/LA update with IMSI attach requested, or if the LA changed with the routeing area update, the new SGSN sends a Location Update Request (new LAI, IMSI, SGSN Number, Location Update Type) to the VLR. Location Update Type shall indicate IMSI attach if Update Type in step 1 indicated combined RA/LA update with IMSI attach requested. Otherwise, Location Update Type shall indicate normal location update. When the SGSN does not provide functionality for the Intra Domain Connection of RAN Nodes to Multiple CN Nodes, the VLR number is derived from the RAI. When the SGSN provides functionality for Intra Domain Connection of RAN Nodes to Multiple CN Nodes, the SGSN uses the RAI and a hash value from the IMSI to determine the VLR number. The SGSN starts the location update procedure towards the new MSC/VLR upon receipt of the first Insert Subscriber Data message from the HLR in step 9). The VLR creates or updates the association with the SGSN by storing SGSN Number.

12) If the subscriber data in the VLR is marked as not confirmed by the HLR, the new VLR informs the HLR. The HLR cancels the old VLR and inserts subscriber data in the new VLR:

a) The new VLR sends an Update Location (new VLR) to the HLR.

b) The HLR cancels the data in the old VLR by sending Cancel Location (IMSI) to the old VLR.

c) The old VLR acknowledges with Cancel Location Ack (IMSI).

d) The HLR sends Insert Subscriber Data (IMSI, subscriber data) to the new VLR.

e) The new VLR acknowledges with Insert Subscriber Data Ack (IMSI).

f) The HLR responds with Update Location Ack (IMSI) to the new VLR.

13) The new VLR allocates a new TMSI and responds with Location Update Accept (VLR TMSI) to the SGSN. VLR TMSI is optional if the VLR has not changed.

14) The new SGSN validates the MS's presence in the new RA. If due to roaming restrictions the MS is not allowed to be attached in the RA, or if subscription checking fails, the SGSN rejects the routeing area update with an appropriate cause. If the MS is emergency attached or if the MS has active PDP context(s) for an emergency use, the SGSN should not reject the routing area update due to e.g. roaming restrictions. If all checks are successful, the new SGSN establishes MM and PDP contexts for the MS. A logical link is established between the new SGSN and the MS. The new SGSN responds to the MS with Routeing Area Update Accept (P-TMSI, VLR TMSI, P-TMSI Signature, Receive N-PDU Number). Receive N-PDU Number contains the acknowledgements for each acknowledged-mode NSAPI used by the MS, thereby confirming all mobile-originated N-PDUs successfully transferred before the start of the update procedure.

15) The MS confirms the reallocation of the TMSIs by returning a Routeing Area Update Complete (Receive N-PDU Number) message to the SGSN. Receive N-PDU Number contains the acknowledgements for each acknowledged-mode NSAPI used by the MS, thereby confirming all mobile-terminated N-PDUs successfully transferred before the start of the update procedure. If Receive N-PDU Number confirms reception of N-PDUs that were forwarded from the old SGSN, these N-PDUs shall be discarded by the new SGSN. LLC and SNDCP in the MS are reset.

16) The new SGSN sends a TMSI Reallocation Complete message to the new VLR if the MS confirms the VLR TMSI.

In the case of a rejected routeing area update operation, due to regional subscription or roaming restrictions, or because the SGSN cannot determine the HLR address to establish the locating updating dialogue, the new SGSN shall not construct an MM context. A reject shall be returned to the MS with an appropriate cause. The MS shall not re-attempt a routeing area update to that RA. The RAI value shall be deleted when the MS is powered-up.

If the new SGSN is unable to update the PDP context in one or more GGSNs, the new SGSN shall deactivate the corresponding PDP contexts as described in clause "SGSN-initiated PDP Context Deactivation Procedure". This shall not cause the SGSN to reject the routeing area update.

The PDP Contexts shall be sent from old to new SGSN in a prioritized order, i.e. the most important PDP Context first in the SGSN Context Response message. (The prioritization method is implementation dependent, but should be based on the current activity.)

If the new SGSN is unable to support the same number of active PDP contexts as received from old SGSN, the new SGSN should use the prioritisation sent by old SGSN as input when deciding which PDP contexts to maintain active and which ones to delete. PDP contexts related to an emergency use shall have a high priority and therefore PDP contexts for emergency use should not be deactivated during the routeing area update. In any case, the new SGSN shall first update all contexts in one or more GGSNs and then deactivate the context(s) that it cannot maintain as described in subclause "SGSN-initiated PDP Context Deactivation Procedure". This shall not cause the SGSN to reject the routeing area update.

If the routeing area update procedure fails a maximum allowable number of times, or if the SGSN returns a Routeing Area Update Reject (Cause) message, the MS shall enter IDLE state.

If the timer described in step 2 expires and no Cancel Location (IMSI) was received from the HLR, the old SGSN shall stop forwarding N-PDUs to the new SGSN.

If the Location Update Accept message indicates a reject, this should be indicated to the MS, and the MS shall not access non-GPRS services until a successful location update is performed.

The CAMEL procedure calls shall be performed, see referenced procedures in TS 23.078:

C1) CAMEL_GPRS_PDP_Context_Disconnection, CAMEL_GPRS_Detach and CAMEL_PS_Notification.

They are called in the following order:

- The CAMEL_GPRS_PDP_Context_Disconnection procedure is called several times: once per PDP context. The procedure returns as result "Continue".
- Then the CAMEL_GPRS_Detach procedure is called once. The procedure returns as result "Continue".
- Then the CAMEL_PS_Notification procedure is called once. The procedure returns as result "Continue".

C2) CAMEL_GPRS_Routeing_Area_Update_Session and CAMEL_PS_Notification.

They are called in the following order:

- The CAMEL_GPRS_Routeing_Area_Update_Session procedure is called. The procedure returns as result "Continue".
- Then the CAMEL_PS_Notification procedure is called. The procedure returns as result "Continue".

C3) CAMEL_GPRS_Routeing_Area_Update_Context.

This procedure is called several times: once per PDP context. It returns as result "Continue".

6.2.4 Location Management Procedures (Iu-mode)

6.2.4.1 Routeing Area Update Procedure

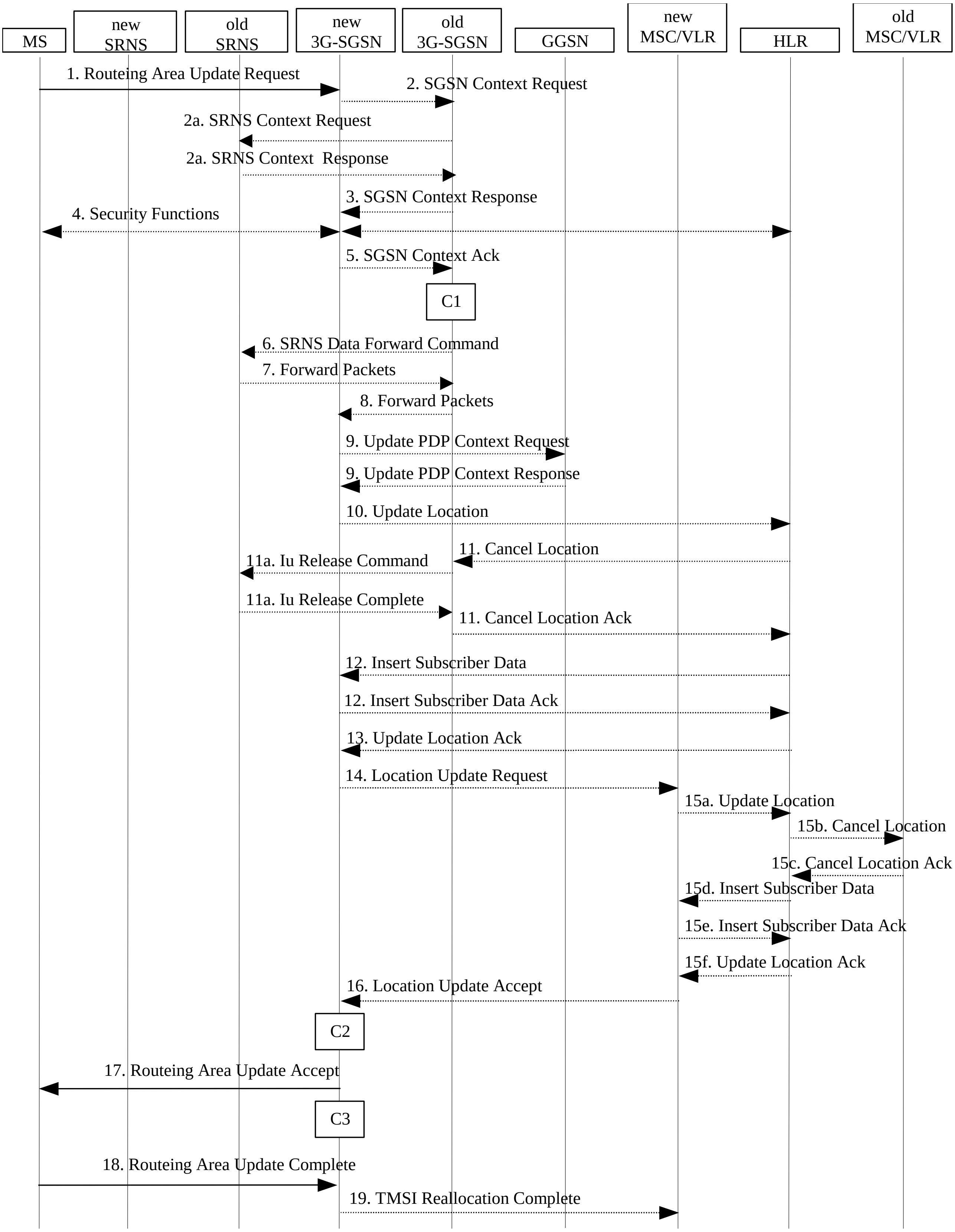

Figure 6.6: Iu mode RA Update Procedure

1) The RRC connection is established, if not already done. The MS sends a Routeing Area Update Request message (P-TMSI, old RAI, old P-TMSI Signature, Update Type, follow on request, Classmark, DRX Parameters, MS Network Capability) to the new SGSN. The MS shall set a follow-on request if there is pending uplink traffic (signalling or user data). The SGSN may use, as an implementation option, the follow-on request indication to release or keep the Iu connection after the completion of the RA update procedure. Update Type shall indicate:

   - RA Update if the RA Update is triggered by a change of RA;

   - Periodic RA Update if the RA update is triggered by the expiry of the Periodic RA Update timer;

   - Combined RA/LA Update if the MS is also IMSI-attached and the LA update shall be performed in network operation mode I (see clause "Interactions Between SGSN and MSC/VLR"); or

   - Combined RA/LA Update with IMSI attach requested if the MS wants to perform an IMSI attach in network operation mode I.

   The SRNC shall add the Routeing Area Identity including the RAC and LAC of the area where the MS is located before forwarding the message to the 3G-SGSN. This RA identity corresponds to the RAI in the MM system information sent by the SRNC to the MS. Classmark is described in clause "MS Network Capability". DRX Parameters indicates whether or not the MS uses discontinuous reception and the DRX cycle length.

NOTE 2: Sending the Routeing Area Update Request message to the SGSN triggers the establishment of a signalling connection between RAN and SGSN for the concerned MS.

2) If the RA update is an Inter-SGSN Routeing area update and if the MS was in PMM-IDLE state, the new SGSN sends an SGSN Context Request message (old P-TMSI, old RAI, old P-TMSI Signature) to the old SGSN to get the MM and PDP contexts for the MS. If the new SGSN provides functionality for Intra Domain Connection of RAN Nodes to Multiple CN Nodes, the new SGSN may derive the old SGSN from the old RAI and the old P-TMSI and send the SGSN Context Request message to this old SGSN. Otherwise, the new SGSN derives the old SGSN from the old RAI. In any case the new SGSN will derive an SGSN that it believes is the old SGSN. This derived SGSN is itself the old SGSN, or it is associated with the same pool area as the actual old SGSN and it will determine the correct old SGSN from the P-TMSI and relay the message to that actual old SGSN. The old SGSN validates the old P-TMSI Signature and responds with an appropriate error cause if it does not match the value stored in the old SGSN. This should initiate the security functions in the new SGSN. If the security functions authenticate the MS correctly, the new SGSN shall send an SGSN Context Request (IMSI, old RAI, MS Validated) message to the old SGSN. MS Validated indicates that the new SGSN has authenticated the MS. If the old P-TMSI Signature was valid or if the new SGSN indicates that it has authenticated the MS, the old SGSN starts a timer.. If the MS is not known in the old SGSN, the old SGSN responds with an appropriate error cause.

2a) If the MS is PMM-CONNECTED state in the old 3G-SGSN or, in case of an intra-SGSN RA update, if the MS is in the PMM-CONNECTED state and the RAU was received over another Iu connection than the established one, the old SGSN sends an SRNS Context Request (IMSI) message to the old SRNS to retrieve the sequence numbers for the PDP context for inclusion in the SGSN Context Response message. Upon reception of this message, the SRNS buffers and stops sending downlink PDUs to the MS and returns an SRNS Context Response (IMSI, GTP-SNDs, GTP-SNUs, PDCP-SNUs) message. The SRNS shall include for each PDP context the next in-sequence GTP sequence number to be sent to the MS and the GTP sequence number of the next uplink PDU to be tunnelled to the GGSN. For each active PDP context which uses lossless PDCP, the SRNS also includes the uplink PDCP sequence number (PDCP-SNU). PDCP-SNU shall be the next in-sequence PDCP sequence number expected from the MS (per each active radio bearer). No conversion of PDCP sequence numbers to SNDCP sequence numbers shall be done in the 3G-SGSN.

3) The old 3G-SGSN responds with an SGSN Context Response (MM Context, PDP Contexts) message. For each PDP context the old 3G-SGSN shall include the GTP sequence number for the next uplink GTP PDU to be tunnelled to the GGSN and the next downlink GTP sequence number for the next PDU to be sent to the MS. Each PDP Context also includes the PDCP sequence numbers if PDCP sequence numbers are received from the old SRNS. The new 3G-SGSN shall ignore the MS Network Capability contained in MM Context of SGSN Context Response only when it has previously received an MS Network Capability in the Routeing Area Request. The GTP sequence numbers received from the old 3G-SGSN are only relevant if delivery order is required for the PDP context (QoS profile).

4) Security functions may be executed. These procedures are defined in clause "Security Function". If the SGSN Context Response message did not include IMEISV and ADD is supported, the SGSN retrieves the IMEISV from the MS. If the security functions do not authenticate the MS correctly, the routeing area update shall be

rejected, and the new SGSN shall send a reject indication to the old SGSN. The old SGSN shall continue as if the SGSN Context Request was never received. If the MS is emergency attached or if the MS has active PDP context(s) for an emergency use (i.e. PDP context(s) with a globally dedicated emergency APN), the SGSN should not reject the routing area update due to authentication failure. However, the SGSN may reject the routing area update based on national regulatory requirements.

5) If the RA update is an Inter-SGSN Routeing area update, the new SGSN sends an SGSN Context Acknowledge message to the old SGSN. The old SGSN marks in its context that the MSC/VLR association and the information in the GGSNs and the HLR are invalid. This triggers the MSC/VLR, the GGSNs, and the HLR to be updated if the MS initiates a routeing area update procedure back to the old SGSN before completing the ongoing routeing area update procedure.

6) If the MS is in PMM-CONNECTED state in the old 3G-SGSN or, in case of an intra-SGSN RA update, if the MS is PMM connected and the RAU was received over another Iu connection than the established one, the old 3G-SGSN sends an SRNS Data Forward Command (RAB ID, Transport Layer Address, Iu Transport Association) message to the SRNS. Upon receipt of the SRNS Data Forward Command message from the 3G-SGSN, the SRNS shall start the data-forwarding timer.

7) For each indicated RAB the SRNS starts duplicating and tunnelling the buffered GTP PDUs to the old 3G-SGSN. For each radio bearer which uses lossless PDCP the SRNS shall start tunnelling the partly transmitted and the transmitted but not acknowledged PDCP-PDUs together with their related PDCP sequence numbers and start duplicating and tunnelling the buffered GTP PDUs to the old 3G-SGSN. Upon receipt of the SRNS Data Forward Command message from the 3G-SGSN, the SRNS shall start the data-forwarding timer.

8) If the RA update is an Inter-SGSN RA Update, the old 3G-SGSN tunnels the GTP PDUs to the new 3G-SGSN. No conversion of PDCP sequence numbers to SNDCP sequence numbers shall be done in the 3G-SGSN.

9) If the RA update is an Inter-SGSN RA Update and if the MS was not in PMM-CONNECTED state in the new 3G-SGSN, the new SGSN sends Update PDP Context Request (new SGSN Address, QoS Negotiated, Tunnel Endpoint Identifier, serving network identity, CGI/SAI, RAT type) to the GGSNs concerned. The SGSN shall send the serving network identity to the GGSN. The GGSNs update their PDP context fields and return an Update PDP Context Response (Tunnel Endpoint Identifier, Prohibit Payload Compression, APN Restriction). The Prohibit Payload Compression indicates that the SGSN should negotiate no data compression for this PDP context. Note: If the RA update is an Inter-SGSN routeing area update initiated by an MS in PMM-CONNECTED state in the new 3G-SGSN, the Update PDP Context Request message is sent as described in subclause "Serving RNS Relocation Procedures".

10) If the RA update is an Inter-SGSN RA Update, the new SGSN informs the HLR of the change of SGSN by sending Update Location (SGSN Number, SGSN Address, IMSI, IMEISV) to the HLR. IMEISV is sent if the ADD function is supported.

11) If the RA update is an Inter-SGSN RA Update, the HLR sends Cancel Location (IMSI, Cancellation Type) to the old SGSN with Cancellation Type set to Update Procedure. If the timer described in step 2 is not running, the old SGSN removes the MM context. Otherwise, the contexts are removed only when the timer expires. It also ensures that the MM context is kept in the old SGSN in case the MS initiates another inter SGSN routeing area update before completing the ongoing routeing area update to the new SGSN. The old SGSN acknowledges with Cancel Location Ack (IMSI).

11a) On receipt of Cancel Location, if the MS is PMM-CONNECTED in the old 3G-SGSN, the old 3G-SGSN sends an Iu Release Command message to the old SRNC. When the data-forwarding timer has expired, the SRNS responds with an Iu Release Complete message.

12) If the RA update is an inter-SGSN RA Update, the HLR sends Insert Subscriber Data (IMSI, subscription data) to the new SGSN. The new SGSN validates the MS's presence in the (new) RA. If due to regional subscription restrictions or access restrictions the MS is not allowed to be attached in the RA, the SGSN rejects the Routeing Area Update Request with an appropriate cause, and may return an Insert Subscriber Data Ack (IMSI, SGSN Area Restricted) message to the HLR. If all checks are successful, the SGSN constructs an MM context for the MS and returns an Insert Subscriber Data Ack (IMSI) message to the HLR.

13) If the RA update is an Inter-SGSN RA Update, the HLR acknowledges the Update Location by sending Update Location Ack (IMSI) to the new SGSN.

14) If Update Type indicates combined RA/LA update with IMSI attach requested, or if the LA changed with the routeing area update, the association has to be established, and the new SGSN sends a Location Update Request (new LAI, IMSI, SGSN Number, Location Update Type) to the VLR. Location Update Type shall indicate IMSI attach if Update Type in step 1 indicated combined RA/LA update with ISI attach requested. Otherwise, Location Update Type shall indicate normal location update. When the SGSN does not provide functionality for the Intra Domain Connection of RAN Nodes to Multiple CN Nodes, the VLR number is derived from the RAI. When the SGSN provides functionality for Intra Domain Connection of RAN Nodes to Multiple CN Nodes, the SGSN uses the RAI and a hash value from the IMSI to determine the VLR number. The SGSN starts the location update procedure towards the new MSC/VLR upon receipt of the first Insert Subscriber Data message from the HLR in step 8). The VLR creates or updates the association with the SGSN by storing SGSN Number.

15) If the subscriber data in the VLR is marked as not confirmed by the HLR, the new VLR informs the HLR. The HLR cancels the old VLR and inserts subscriber data in the new VLR:

    a) The new VLR sends an Update Location (new VLR) to the HLR.

    b) The HLR cancels the data in the old VLR by sending Cancel Location (IMSI) to the old VLR.

    c) The old VLR acknowledges with Cancel Location Ack (IMSI).

    d) The HLR sends Insert Subscriber Data (IMSI, subscriber data) to the new VLR.

    e) The new VLR acknowledges with Insert Subscriber Data Ack (IMSI).

    f) The HLR responds with Update Location Ack (IMSI) to the new VLR.

16) The new VLR allocates a new TMSI and responds with Location Update Accept (VLR TMSI) to the SGSN. VLR TMSI is optional if the VLR has not changed.

17) The new SGSN validates the MS's presence in the new RA. If due to roaming restrictions or access restrictions the MS is not allowed to be attached in the RA, or if subscription checking fails, the SGSN rejects the routeing area update with an appropriate cause. If the MS is emergency attached or if the MS has active PDP context(s) for an emergency use (i.e. PDP context(s) with a globally dedicated emergency APN), the SGSN should not reject the routing area update due to e.g. roaming restrictions. If all checks are successful, the new SGSN establishes MM context for the MS. The new SGSN responds to the MS with Routeing Area Update Accept (P-TMSI, VLR TMSI, P-TMSI Signature).

18) The MS confirms the reallocation of the TMSIs by returning a Routeing Area Update Complete message to the SGSN.

19) The new SGSN sends a TMSI Reallocation Complete message to the new VLR if the MS confirms the VLR TMSI.

NOTE 3: Steps 15, 16, and 19 are performed only if step 14 is performed.

NOTE 4: The new SGSN may initiate RAB establishment after execution of the security functions (step 4), or wait until completion of the RA update procedure. For the MS, RAB establishment may occur anytime after the RA update request is sent (step 1).

In the case of a rejected routeing area update operation, due to regional subscription, roaming restrictions, or access restrictions (see TS 23.221 and TS 23.008) the new SGSN shall not construct an MM context. A reject shall be returned to the MS with an appropriate cause. The MS shall not re-attempt a routeing area update to that RA. The RAI value shall be deleted when the MS is powered up.

If the new SGSN is unable to update the PDP context in one or more GGSNs, the new SGSN shall deactivate the corresponding PDP contexts as described in subclause "SGSN-initiated PDP Context Deactivation Procedure". This shall not cause the SGSN to reject the routeing area update.

The PDP Contexts shall be sent from old to new SGSN in a prioritized order, i.e. the most important PDP Context first in the SGSN Context Response message. (The prioritization method is implementation dependent, but should be based on the current activity.)

PDP contexts for emergency use (i.e. PDP context(s) with a globally dedicated emergency APN) shall have a high priority and therefore PDP contexts for emergency use should not be deactivated during the routing area update.

The new SGSN shall determine the Maximum APN restriction based on the received APN Restriction of each PDP context from the GGSN and then store the new Maximum APN restriction value.

If the new SGSN is unable to support the same number of active PDP contexts as received from old SGSN, the new SGSN should use the prioritisation sent by old SGSN as input when deciding which PDP contexts to maintain active and which ones to delete. In any case, the new SGSN shall first update all contexts in one or more GGSNs and then deactivate the context(s) that it cannot maintain as described in subclause "SGSN-initiated PDP Context Deactivation Procedure". This shall not cause the SGSN to reject the routeing area update.

NOTE 5: In case MS was in PMM-CONNECTED state the PDP Contexts are sent already in the Forward Relocation Request message as described in subclause "Serving RNS relocation procedures".

If the routeing area update procedure fails a maximum allowable number of times, or if the SGSN returns a Routeing Area Update Reject (Cause) message, the MS shall enter PMM-DETACHED state.

If the Location Update Accept message indicates a reject, this should be indicated to the MS, and the MS shall not access non-PS services until a successful location update is performed.

The CAMEL procedure calls shall be performed, see referenced procedures in TS 23.078:

C1) CAMEL_GPRS_PDP_Context_Disconnection, CAMEL_GPRS_Detach and CAMEL_PS_Notification.

They are called in the following order:

- The CAMEL_GPRS_PDP_Context_Disconnection procedure is called several times: once per PDP context. The procedure returns as result "Continue".
- Then the CAMEL_GPRS_Detach procedure is called once. The procedure returns as result "Continue".
- Then the CAMEL_PS_Notification procedure is called once. The procedure returns as result "Continue".

C2) CAMEL_GPRS_Routeing_Area_Update_Session and CAMEL_PS_Notification.

They are called in the following order:

- The CAMEL_GPRS_Routeing_Area_Update_Session procedure is called. The procedure returns as result "Continue".
- Then the CAMEL_PS_Notification procedure is called. The procedure returns as result "Continue".

C3) CAMEL_GPRS_Routeing_Area_Update_Context.

This procedure is called several times: once per PDP context. It returns as result "Continue".

NOTE 6: It is FFS whether CAMEL procedures are performed if the MS is emergency attached or if the MS has active PDP context(s) for an emergency use.

6.2.4.2 Serving RNS Relocation Procedures

6.2.4.2.1 Serving RNS Relocation Procedure

The Serving SRNS Relocation procedure is illustrated in Figure 6.7. The sequence is valid for both intra-SGSN SRNS relocation and inter-SGSN SRNS relocation.

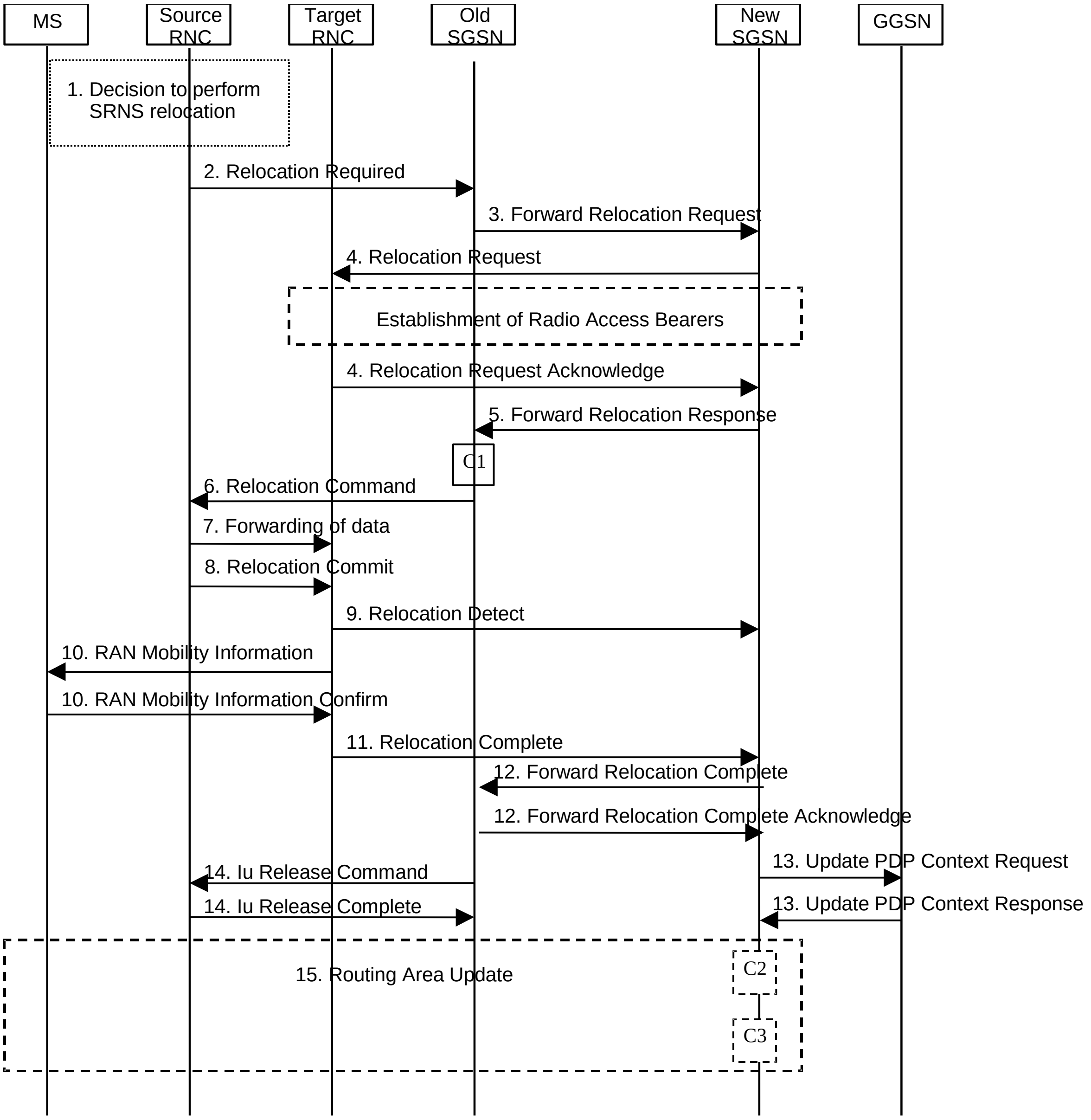
MS
Source RNC
Target RNC
Old SGSN
New SGSN
GGSN
1. Decision to perform SRNS relocation
2. Relocation Required
3. Forward Relocation Request
4. Relocation Request
Establishment of Radio Access Bearers
4. Relocation Request Acknowledge
5. Forward Relocation Response
C1
6. Relocation Command
7. Forwarding of data
8. Relocation Commit
9. Relocation Detect
10. RAN Mobility Information
10. RAN Mobility Information Confirm
11. Relocation Complete
12. Forward Relocation Complete
12. Forward Relocation Complete Acknowledge
13. Update PDP Context Request
14. Iu Release Command
14. Iu Release Complete
13. Update PDP Context Response
15. Routing Area Update
C2
C3

Figure 6.7: SRNS Relocation Procedure

1) The source SRNC decides to perform/initiate SRNS relocation. At this point both uplink and downlink user data flows via the following tunnel(s): Radio Bearer between MS and source SRNC (data flows via the target RNC, which acts as a drift RNC); GTP-U tunnel(s) between source SRNC and old-SGSN; GTP-U tunnel(s) between old-SGSN and GGSN.

2) The source SRNC sends a Relocation Required message (Relocation Type, Cause, Source ID, Target ID, Source RNC to target RNC transparent container) to the old SGSN. The source SRNC shall set the Relocation Type to "UE not involved". The Source SRNC to Target RNC Transparent Container includes the necessary information for Relocation co-ordination, security functionality and RRC protocol context information (including MS Capabilities).

3) The old SGSN determines from the Target ID if the SRNS Relocation is intra-SGSN SRNS relocation or inter-SGSN SRNS relocation. In case of inter-SGSN SRNS relocation, the old SGSN initiates the relocation resource

allocation procedure by sending a Forward Relocation Request message (IMSI, Tunnel Endpoint Identifier Signalling, MM Context, PDP Context, Target Identification, RAN transparent container, RANAP Cause) to the new SGSN. For relocation to an area where Intra Domain Connection of RAN Nodes to Multiple CN Nodes is used, the old SGSN may – if it provides Intra Domain Connection of RAN Nodes to Multiple CN Nodes -have multiple target SGSNs for each relocation target in a pool area, in which case the old SGSN will select one of them to become the new SGSN, as specified in TS 23.236 [73]. The PDP context contains GGSN Address for User Plane and Uplink TEID for Data (to this GGSN Address and Uplink TEID for Data the old SGSN and the new SGSN send uplink packets). At the same time a timer is started on the MM and PDP contexts in the old SGSN (see the Routeing Area Update procedure in subclause "Location Management Procedures (Iu mode)"). The Forward Relocation Request message is applicable only in the case of inter-SGSN SRNS relocation.

4) The new SGSN sends a Relocation Request message (Permanent NAS UE Identity, Cause, CN Domain Indicator, Source-RNC to target RNC transparent container, RABs to be setup) to the target RNC. Only the Iu Bearers of the RABs are setup between the target RNC and the new-SGSN as the existing Radio Bearers will be reallocated between the MS and the target RNC when the target RNC takes the role of the serving RNC. For each requested RAB, the RABs to be setup information elements shall contain information such as RAB ID, RAB parameters, Transport Layer Address, and Iu Transport Association. SGSN shall not establish RABs for PDP contexts with maximum bitrate for uplink and downlink of 0 kbit/s. The RAB ID information element contains the NSAPI value, and the RAB parameters information element gives the QoS profile. The Transport Layer Address is the SGSN Address for user data, and the Iu Transport Association corresponds to the uplink Tunnel Endpoint Identifier Data. After all necessary resources for accepted RABs including the Iu user plane are successfully allocated; the target RNC shall send the Relocation Request Acknowledge message (RABs setup, RABs failed to setup) to the new SGSN. Each RAB to be setup is defined by a Transport Layer Address, which is the target RNC Address for user data, and an Iu Transport Association, which corresponds to the downlink Tunnel Endpoint Identifier for user data. For each RAB to be set up, the target RNC may receive simultaneously downlink user packets both from the source SRNC and from the new SGSN.

5) When resources for the transmission of user data between the target RNC and the new SGSN have been allocated and the new SGSN is ready for relocation of SRNS, the Forward Relocation Response message (Cause, RANAP Cause, and RAB Setup Information) is sent from the new SGSN to old SGSN. This message indicates that the target RNC is ready to receive from source SRNC the forwarded downlink PDUs, i.e. the relocation resource allocation procedure is terminated successfully. RANAP Cause is information from the target RNC to be forwarded to the source SRNC. The RAB Setup Information, one information element for each RAB, contains the RNC Tunnel Endpoint Identifier and the RNC IP address for data forwarding from the source SRNC to the target RNC. If the target RNC or the new SGSN failed to allocate resources, the RAB Setup Information element contains only NSAPI indicating that the source SRNC shall release the resources associated with the NSAPI.PDP contexts for emergency use (i.e. PDP context(s) with a globally dedicated emergency APN) shall have a high priority and therefore RABs for PDP contexts for emergency use should not be dropped in the SGSN during SRNS relocation procedure The Forward Relocation Response message is applicable only in case of inter-SGSN SRNS relocation.

6) The old SGSN continues the relocation of SRNS by sending a Relocation Command message (RABs to be released, and RABs subject to data forwarding) to the source SRNC. The old SGSN decides the RABs to be subject for data forwarding based on QoS, and those RABs shall be contained in RABs subject to data forwarding. For each RAB subject to data forwarding, the information element shall contain RAB ID, Transport Layer Address, and Iu Transport Association. These are the same Transport Layer Address and Iu Transport Association that the target RNC had sent to new SGSN in Relocation Request Acknowledge message, and these are used for forwarding of downlink N-PDU from source SRNC to target RNC. The source SRNC is now ready to forward downlink user data directly to the target RNC over the Iu interface. This forwarding is performed for downlink user data only.

7) The source SRNC may, according to the QoS profile, begin the forwarding of data for the RABs to be subject for data forwarding. The data forwarding at SRNS relocation shall be carried out through the Iu interface, meaning that the data exchanged between the source SRNC and the target RNC are duplicated in the source SRNC and routed at IP layer towards the target RNC. For each radio bearer which uses lossless PDCP the GTP-PDUs related to transmitted but not yet acknowledged PDCP-PDUs are duplicated and routed at IP layer towards the target RNC together with their related downlink PDCP sequence numbers. The source RNC continues transmitting duplicates of downlink data and receiving uplink data. Before the serving RNC role is not yet taken over by target RNC and when downlink user plane data starts to arrive to target RNC, the target RNC may buffer or discard arriving downlink GTP-PDUs according to the related QoS profile.

NOTE: The order of steps, starting from step 7 onwards, does not necessarily reflect the order of events. For instance, source RNC may start data forwarding (step 7) and send Relocation Commit message (step 8) almost simultaneously except in the delivery order required case where step 7 triggers step 8. Target RNC may send Relocation Detect message (step 9) and RAN Mobility Information message (step 10) at the same time. Hence, target RNC may receive RAN Mobility Information Confirm message (step 10) while data forwarding (step 7) is still underway, and before the new SGSN receives Update PDP Context Response message (step 11).

8) Before sending the Relocation Commit the uplink and downlink data transfer in the source, SRNC shall be suspended for RABs, which require delivery order. The source RNC shall start the data-forwarding timer. When the source SRNC is ready, the source SRNC shall trigger the execution of relocation of SRNS by sending a Relocation Commit message (SRNS Contexts) to the target RNC over the Iur interface. The purpose of this procedure is to transfer SRNS contexts from the source RNC to the target RNC, and to move the SRNS role from the source RNC to the target RNC. SRNS contexts are sent for each concerned RAB and contain the sequence numbers of the GTP-PDUs next to be transmitted in the uplink and downlink directions and the next PDCP sequence numbers that would have been used to send and receive data from the MS. For PDP context(s) using delivery order not required (QoS profile), the sequence numbers of the GTP-PDUs next to be transmitted are not used by the target RNC. PDCP sequence numbers are only sent by the source RNC for radio bearers, which used lossless PDCP [57]. The use of lossless PDCP is selected by the RNC when the radio bearer is set up or reconfigured.

   If delivery order is required (QoS profile), consecutive GTP-PDU sequence numbering shall be maintained throughout the lifetime of the PDP context(s). Therefore, during the entire SRNS relocation procedure for the PDP context(s) using delivery order required (QoS profile), the responsible GTP-U entities (RNCs and GGSN) shall assign consecutive GTP-PDU sequence numbers to user packets belonging to the same PDP context for uplink and downlink, respectively.

9) The target RNC shall send a Relocation Detect message to the new SGSN when the relocation execution trigger is received. For SRNS relocation type "UE not involved", the relocation execution trigger is the reception of the Relocation Commit message from the Iur interface. When the Relocation Detect message is sent, the target RNC shall start SRNC operation.

10) The target SRNC sends a RAN Mobility Information message. This message contains UE information elements and CN information elements. The UE information elements include among others new SRNC identity and S-RNTI. The CN information elements contain among others Location Area Identification and Routeing Area Identification. The procedure shall be co-ordinated in all Iu signalling connections existing for the MS.

   The target SRNC establishes and/or restarts the RLC, and exchanges the PDCP sequence numbers (PDCP-SNU, PDCP-SND) between the target SRNC and the MS. PDCP-SND is the PDCP sequence number for the next expected in-sequence downlink packet to be received in the MS per radio bearer, which used lossless PDCP in the source RNC. PDCP-SND confirms all mobile-terminated packets successfully transferred before the SRNC relocation. If PDCP-SND confirms reception of packets that were forwarded from the source SRNC, the target SRNC shall discard these packets. PDCP-SNU is the PDCP sequence number for the next expected in-sequence uplink packet to be received in the RNC per radio bearer, which used lossless PDCP in the source RNC. PDCP-SNU confirms all mobile originated packets successfully transferred before the SRNC relocation. If PDCP-SNU confirms reception of packets that were received in the source SRNC, the MS shall discard these packets.

   Upon reception of the RAN Mobility Information message the MS may start sending uplink user data to the target SRNC. When the MS has reconfigured itself, it sends the RAN Mobility Information Confirm message to the target SRNC. This indicates that the MS is also ready to receive downlink data from the target SRNC.

   If new the SGSN has already received the Update PDP Context Response message from the GGSN, it shall forward the uplink user data to GGSN over this new GTP-U tunnel. Otherwise, the new SGSN shall forward the uplink user data to that GGSN IP address and TEID(s), which the new SGSN had received earlier by the Forward Relocation Request message.

   For all RABs, the target RNC should:

   - start uplink reception of data and start transmission of uplink GTP-PDUs towards the new SGSN;
   - start processing the already buffered and the arriving downlink GTP-PDUs and start downlink transmission towards the MS.

11) When the target SRNC receives the RAN Mobility Information Confirm message, i.e. the new SRNC—ID + S-RNTI are successfully exchanged with the MS by the radio protocols, the target SRNC shall initiate the Relocation Complete procedure by sending the Relocation Complete message to the new SGSN. The purpose of the Relocation Complete procedure is to indicate by the target SRNC the completion of the relocation of the SRNS to the CN.

    Upon receipt of Relocation Complete message, if the SRNS Relocation is an inter SGSN SRNS relocation, the new SGSN signals to the old SGSN the completion of the SRNS relocation procedure by sending a Forward Relocation Complete message.

    Upon receipt of the Relocation Complete message, the CN shall switch the user plane from the source RNC to the target SRNC. If the SRNS Relocation is an inter-SGSN SRNS relocation, the new SGSN sends Update PDP Context Request messages (new SGSN Address, SGSN Tunnel Endpoint Identifier, QoS Negotiated, serving network identity, CGI/SAI, RAT type) to the GGSNs concerned. The SGSN shall send the serving network identity to the GGSN. The GGSNs update their PDP context fields and return an Update PDP Context Response (GGSN Tunnel Endpoint Identifier, Prohibit Payload Compression, APN Restriction) message. The Prohibit Payload Compression indicates that the SGSN should negotiate no data compression for this PDP context.

14) Upon receiving the Relocation Complete message or if it is an inter-SGSN SRNS relocation; the Forward Relocation Complete message, the old SGSN sends an Iu Release Command message to the source RNC. When the RNC data-forwarding timer has expired the source RNC responds with an Iu Release Complete.

15) After the MS has finished the RNTI reallocation procedure and if the new Routeing Area Identification is different from the old one, the MS initiates the Routeing Area Update procedure. See subclause "Location Management Procedures (Iu mode)". Note that it is only a subset of the RA update procedure that is performed, since the MS is in PMM-CONNECTED mode.

    The new SGSN shall determine the Maximum APN restriction based on the received APN Restriction of each PDP context from the GGSN and then store the new Maximum APN restriction value.

    If the SRNS Relocation is inter-SGSN, then the following CAMEL procedure calls shall be performed (see referenced procedures in TS 23.078)

C1) CAMEL_GPRS_PDP_Context_Disconnection, CAMEL_GPRS_Detach and CAMEL_PS_Notification.

They are called in the following order:

- The CAMEL_GPRS_PDP_Context_Disconnection procedure is called several times: once per PDP context. The procedure returns as result "Continue".
- Then the CAMEL_GPRS_Detach procedure is called once. The procedure returns as result "Continue".
- Then the CAMEL_PS_Notification procedure is called once. The procedure returns as result "Continue".

If the SRNS Relocation is intra-SGSN, then the above mentioned CAMEL procedures calls shall not be performed.

If Routeing Area Update occurs, then the following CAMEL procedure calls shall be performed (see referenced procedures in TS 23.078):

C2) CAMEL_GPRS_Routeing_Area_Update_Session and CAMEL_PS_Notification.

They are called in the following order:

- The CAMEL_GPRS_Routeing_Area_Update_Session procedure is called. The procedure returns as result "Continue".
- Then, the CAMEL_PS_Notification procedure is called. The procedure returns as result "Continue".

C3) CAMEL_GPRS_Routeing_Area_Update_Context.

This procedure is called several times: once per PDP context. It returns as result ""Continue"".

For C2 and C3: refer to Routing Area Update procedure description for detailed message flow.

NOTE: It is FFS whether CAMEL procedures are performed if the MS is emergency attached or if the MS has active PDP context(s) for an emergency use.

6.2.4.2.2 Combined Hard Handover and SRNS Relocation Procedure

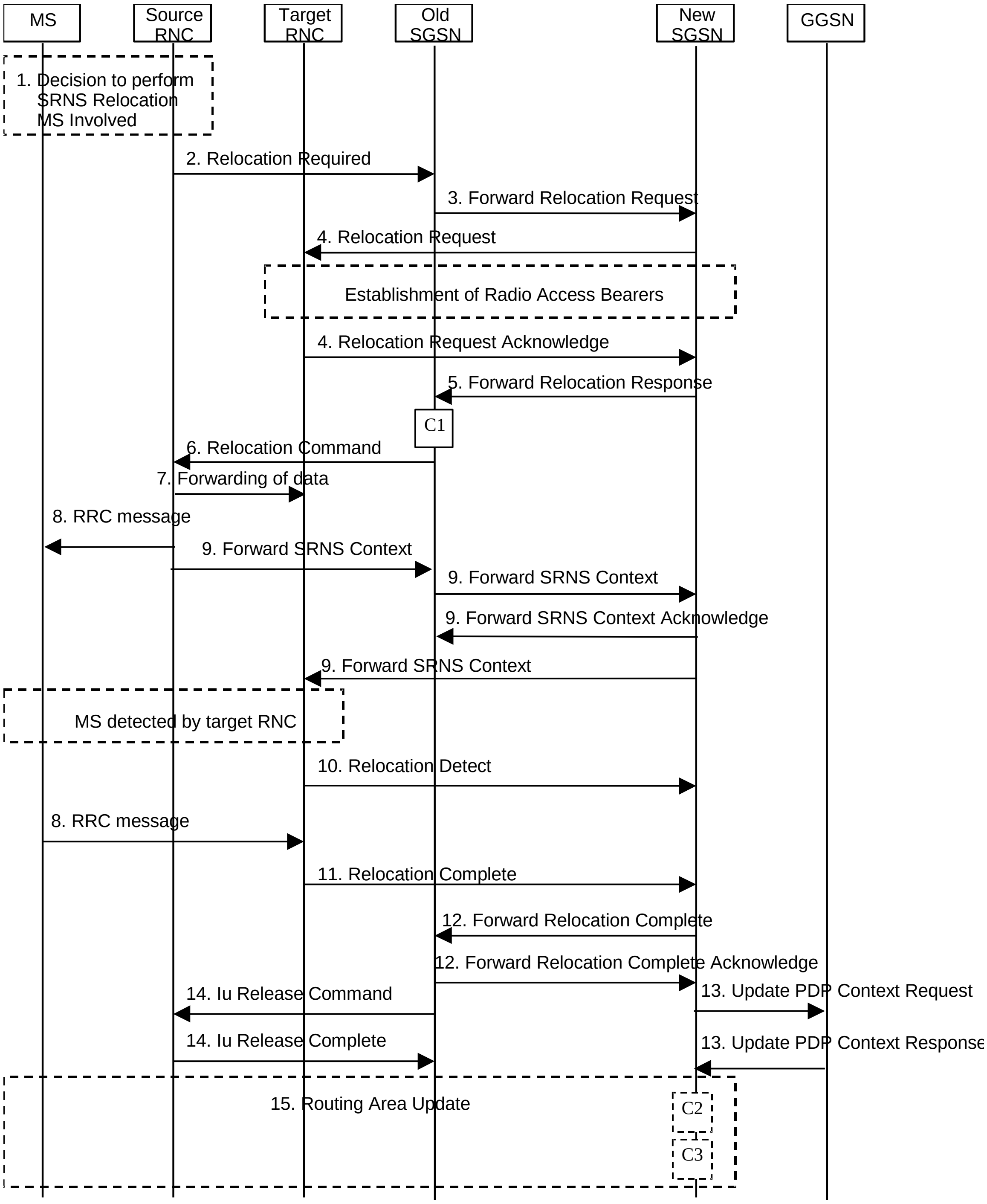
MS
Source RNC
Target RNC
Old SGSN
New SGSN
GGSN
1. Decision to perform SRNS Relocation MS Involved
2. Relocation Required
3. Forward Relocation Request
4. Relocation Request
Establishment of Radio Access Bearers
4. Relocation Request Acknowledge
5. Forward Relocation Response
C1
6. Relocation Command
7. Forwarding of data
8. RRC message
9. Forward SRNS Context
9. Forward SRNS Context
9. Forward SRNS Context Acknowledge
9. Forward SRNS Context
MS detected by target RNC
10. Relocation Detect
8. RRC message
11. Relocation Complete
12. Forward Relocation Complete
12. Forward Relocation Complete Acknowledge
13. Update PDP Context Request
14. Iu Release Command
14. Iu Release Complete
13. Update PDP Context Response
15. Routing Area Update
C2
C3

Figure 6.8: Combined Hard Handover and SRNS Relocation Procedure

1) Based on measurement results and knowledge of the RAN topology, the source SRNC decides to initiate a combined hard handover and SRNS relocation. At this point both uplink and downlink user data flows via the following tunnel(s): Radio Bearer between the MS and the source SRNC (no drift RNC available); GTP-U tunnel(s) between the source SRNC and the old SGSN; GTP-U tunnel(s) between the old SGSN and the GGSN.

2) The source SRNC sends a Relocation Required message (Relocation Type, Cause, Source ID, Target ID, Source RNC To Target RNC Transparent Container) to the old SGSN. The source SRNC shall set Relocation Type to "UE Involved". Source RNC To Target RNC Transparent Container includes the necessary information for relocation co-ordination, security functionality and RRC protocol context information (including MS Capabilities).

3) The old SGSN determines from the Target ID if the SRNS relocation is intra-SGSN SRNS relocation or inter-SGSN SRNS relocation. In case of inter-SGSN SRNS relocation the old SGSN initiates the relocation resource allocation procedure by sending a Forward Relocation Request message (IMSI, Tunnel Endpoint Identifier Signalling, MM Context, PDP Context, Target Identification, RAN Transparent Container, RANAP Cause) to the new SGSN. For relocation to an area where Intra Domain Connection of RAN Nodes to Multiple CN Nodes is used, the old SGSN may – if it provides Intra Domain Connection of RAN Nodes to Multiple CN Nodes -have multiple target SGSNs for each relocation target in a pool area, in which case the old SGSN will select one of them to become the new SGSN, as specified in TS 23.236. PDP context contains GGSN Address for User Plane and Uplink TEID for Data (to this GGSN Address and Uplink TEID for Data, the old SGSN and the new SGSN send uplink packets). At the same time a timer is started on the MM and PDP contexts in the old SGSN (see Routeing Area Update procedure in subclause "Location Management Procedures (Iu mode)"). The Forward Relocation Request message is applicable only in case of inter-SGSN SRNS relocation.

4) The new SGSN sends a Relocation Request message (Permanent NAS UE Identity, Cause, CN Domain Indicator, Source RNC To Target RNC Transparent Container, RAB To Be Setup) to the target RNC. For each RAB requested to be established, RABs To Be Setup shall contain information such as RAB ID, RAB parameters, Transport Layer Address, and Iu Transport Association. SGSN shall not establish RABs for PDP contexts with maximum bitrate for uplink and downlink of 0 kbit/s. The RAB ID information element contains the NSAPI value, and the RAB parameters information element gives the QoS profile. The Transport Layer Address is the SGSN Address for user data, and the Iu Transport Association corresponds to the uplink Tunnel Endpoint Identifier Data.

   After all the necessary resources for accepted RABs including the Iu user plane are successfully allocated, the target RNC shall send the Relocation Request Acknowledge message (Target RNC To Source RNC Transparent Container, RABs Setup, RABs Failed To Setup) to the new SGSN. Each RAB to be setup is defined by a Transport Layer Address, which is the target RNC Address for user data, and the Iu Transport Association, which corresponds to the downlink Tunnel Endpoint Identifier for user data. The transparent container contains all radio-related information that the MS needs for the handover, i.e., a complete RRC message (e.g., Physical Channel Reconfiguration in UTRAN case, or Handover From UTRAN, or Handover Command in GERAN Iu mode case) to be sent transparently via CN and source SRNC to the MS. For each RAB to be set up, the target RNC may receive simultaneously downlink user packets both from the source SRNC and from the new SGSN. PDP contexts for emergency use (i.e. PDP context(s) with a globally dedicated emergency APN) shall have a high priority and therefore RABs for PDP contexts for emergency use should not be dropped in the SGSN during SRNS relocation procedure.

5) When resources for the transmission of user data between target RNC and new SGSN have been allocated and the new SGSN is ready for relocation of SRNS, the Forward Relocation Response (Cause, RAN Transparent Container, RANAP Cause, Target-RNC Information) message is sent from the new SGSN to the old SGSN. This message indicates that the target RNC is ready to receive from source SRNC the forwarded downlink PDUs, i.e., the relocation resource allocation procedure is terminated successfully. RAN transparent container and RANAP Cause are information from the target RNC to be forwarded to the source SRNC. The Target RNC Information, one information element for each RAB to be set up, contains the RNC Tunnel Endpoint Identifier and RNC IP address for data forwarding from the source SRNC to the target RNC. The Forward Relocation Response message is applicable only in case of inter-SGSN SRNS relocation.

6) The old SGSN continues the relocation of SRNS by sending a Relocation Command message (Target RNC To Source RNC Transparent Container, RABs To Be Released, RABs Subject To Data Forwarding) to the source SRNC. The old SGSN decides the RABs to be subject for data forwarding based on QoS, and those RABs shall be contained in RABs subject to data forwarding. For each RAB subject to data forwarding, the information element shall contain RAB ID, Transport Layer Address, and Iu Transport Association. These are the same Transport Layer Address and Iu Transport Association that the target RNC had sent to new SGSN in Relocation Request Acknowledge message, and these are used for forwarding of downlink N-PDU from the source SRNC to the target RNC. The source SRNC is now ready to forward downlink user data directly to the target RNC over the Iu interface. This forwarding is performed for downlink user data only.

7) The source SRNC may, according to the QoS profile, begins the forwarding of data for the RABs to be subject for data forwarding.

NOTE: The order of steps, starting from step 7 onwards, does not necessarily reflect the order of events. For instance, source RNC may start data forwarding (step 7), send the RRC message to MS (step 8) and forward SRNS Context message to the old SGSN (step 9) almost simultaneously.

The data forwarding at SRNS relocation shall be carried out through the Iu interface, meaning that the GTP-PDUs exchanged between the source SRNC and the target RNC are duplicated in the source SRNC and routed at the IP layer towards the target RNC. For each radio bearer which uses lossless PDCP the GTP-PDUs related to transmitted but not yet acknowledged PDCP-PDUs are duplicated and routed at IP layer towards the target RNC together with their related downlink PDCP sequence numbers. The source RNC continues transmitting duplicates of downlink data and receiving uplink data.

Before the serving RNC role is not yet taken over by target RNC and when downlink user plane data starts to arrive to target RNC, the target RNC may buffer or discard arriving downlink GTP-PDUs according to the related QoS profile.

8) Before sending the RRC message the uplink and downlink data transfer shall be suspended in the source SRNC for RABs, which require delivery order. The RRC message is for example Physical Channel Reconfiguration for RNS to RNS relocation, or Intersystem to UTRAN Handover for BSS to RNS relocation, or Handover from UTRAN Command for BSS relocation, or Handover Command for BSS to BSS relocation. When the source SRNC is ready, the source RNC shall trigger the execution of relocation of SRNS by sending to the MS the RRC message provided in the Target RNC to source RNC transparent container, e.g., a Physical Channel Reconfiguration (UE Information Elements, CN Information Elements) message. UE Information Elements include among others new SRNC identity and S-RNTI. CN Information Elements contain among others Location Area Identification and Routeing Area Identification.

   When the MS has reconfigured itself, it sends an RRC message e.g., a Physical Channel Reconfiguration Complete message to the target SRNC. If the Forward SRNS Context message with the sequence numbers is received, the exchange of packets with the MS may start. If this message is not yet received, the target RNC may start the packet transfer for all RABs, which do not require maintaining the delivery order.

9) The source SRNC continues the execution of relocation of SRNS by sending a Forward SRNS Context (RAB Contexts) message to the target RNC via the old and the new SGSN. The Forward SRNS Context message is acknowledged by a Forward SRNS Context Acknowledge message, from new to old SGSN. The purpose of this procedure is to transfer SRNS contexts from the source RNC to the target RNC, and to move the SRNS role from the source RNC to the target RNC. SRNS contexts are sent for each concerned RAB and contain the sequence numbers of the GTP PDUs next to be transmitted in the uplink and downlink directions and the next PDCP sequence numbers that would have been used to send and receive data from the MS. PDCP sequence numbers are only sent by the source RNC for the radio bearers which used lossless PDCP [57]. The use of lossless PDCP is selected by the RNC when the radio bearer is set up or reconfigured. For PDP context(s) using delivery order not required (QoS profile), the sequence numbers of the GTP-PDUs next to be transmitted are not used by the target RNC.

   If delivery order is required (QoS profile), consecutive GTP-PDU sequence numbering shall be maintained throughout the lifetime of the PDP context(s). Therefore, during the entire SRNS relocation procedure for the PDP context(s) using delivery order required (QoS profile), the responsible GTP-U entities (RNCs and GGSN) shall assign consecutive GTP-PDU sequence numbers to user packets belonging to the same PDP context uplink and downlink, respectively.

   The target RNC establishes and/or restarts the RLC and exchanges the PDCP sequence numbers (PDCP-SNU, PDCP-SND) between the target RNC and the MS. PDCP-SND is the PDCP sequence number for the next expected in-sequence downlink packet to be received by the MS per radio bearer, which used lossless PDCP in the source RNC. PDCP-SND confirms all mobile terminated packets successfully transferred before the SRNC relocation. If PDCP-SND confirms reception of packets that were forwarded from the source SRNC, then the target SRNC shall discard these packets. PDCP-SNU is the PDCP sequence number for the next expected in-sequence uplink packet to be received in the RNC per radio bearer, which used lossless PDCP in the source RNC. PDCP-SNU confirms all mobile originated packets successfully transferred before the SRNC relocation. If PDCP-SNU confirms reception of packets that were received in the source SRNC, the MS shall discard these packets.

10) The target RNC shall send a Relocation Detect message to the new SGSN when the relocation execution trigger is received. For SRNS relocation type "UE Involved", the relocation execution trigger may be received from the Uu interface; i.e., when target RNC detects the MS on the lower layers. When the Relocation Detect message is sent, the target RNC shall start SRNC operation.

When the target SRNC receives the appropriate RRC message, e.g. Physical Channel Reconfiguration Complete message or the Radio Bearer Release Complete message in UTRAN case, or the Handover To UTRAN Complete message or Handover Complete message in GERAN case, i.e. the new SRNC-ID + S-RNTI are successfully exchanged with the MS by the radio protocols, the target SRNC shall initiate a Relocation Complete procedure by sending the Relocation Complete message to the new SGSN. The purpose of the Relocation Complete procedure is to indicate by the target SRNC the completion of the relocation of the SRNS to the CN.

Upon receipt of Relocation Complete message, if the SRNS Relocation is an inter SGSN SRNS relocation, the new SGSN signals to the old SGSN the completion of the SRNS relocation procedure by sending a Forward Relocation Complete message.

Upon receipt of the Relocation Complete message, the CN shall switch the user plane from the source RNC to the target SRNC. If the SRNS Relocation is an inter-SGSN SRNS relocation, the new SGSN sends Update PDP Context Request messages (new SGSN Address, SGSN Tunnel Endpoint Identifier, QoS Negotiated, serving network identity, CGI/SAI, RAT type) to the GGSNs concerned. The SGSN shall send the serving network identity to the GGSN. The GGSNs update their PDP context fields and return an Update PDP Context Response (GGSN Tunnel Endpoint Identifier, Prohibit Payload Compression, APN Restriction) message. The Prohibit Payload Compression indicates that the SGSN should negotiate no data compression for this PDP context.

14) Upon receiving the Relocation Complete message or, if it is an inter-SGSN SRNS relocation, the Forward Relocation Complete message, the old SGSN sends an Iu Release Command message to the source RNC. When the RNC data-forwarding timer has expired, the source RNC responds with an Iu Release Complete message.

15) After the MS has finished the reconfiguration procedure and if the new Routeing Area Identification is different from the old one, the MS initiates the Routeing Area Update procedure. See subclause "Location Management Procedures (Iu mode)". Note that it is only a subset of the RA update procedure that is performed, since the MS is in PMM-CONNECTED state.

If the SRNS Relocation is inter-SGSN, then the following CAMEL procedure calls shall be performed (see referenced procedures in TS 23.078)

C1) CAMEL_GPRS_PDP_Context_Disconnection, CAMEL_GPRS_Detach and CAMEL_PS_Notification.

They are called in the following order:

- The CAMEL_GPRS_PDP_Context_Disconnection procedure is called several times: once per PDP context. The procedure returns as result "Continue".

- Then the CAMEL_GPRS_Detach procedure is called once. The procedure returns as result "Continue".

- Then the CAMEL_PS_Notification procedure is called once. The procedure returns as result "Continue".

The new SGSN shall determine the Maximum APN restriction based on the received APN Restriction of each PDP context from the GGSN and then store the new Maximum APN restriction value.

If the SRNS Relocation is intra-SGSN, then the above mentioned CAMEL procedures calls shall not be performed.

If Routeing Area Update occurs, then the following CAMEL procedure calls shall be performed (see referenced procedures in TS 23.078):

C2) CAMEL_GPRS_Routeing_Area_Update_Session and CAMEL_PS_Notification.

They are called in the following order:

- The CAMEL_GPRS_Routeing_Area_Update_Session procedure is called. In Figure 6.8, the procedure returns as result "Continue".

- Then the CAMEL_PS_Notification procedure is called. The procedure returns as result "Continue".

C3) CAMEL_GPRS_Routeing_Area_Update_Context.

This procedure is called several times: once per PDP context. It returns as result "Continue".

For C2 and C3: refer to Routing Area Update procedure description for detailed message flow.

NOTE: It is FFS whether CAMEL procedures are performed if the MS is emergency attached or if the MS has active PDP context(s) for an emergency use.

6.2.4.2.3 Combined Cell/URA Update and SRNS Relocation Procedure

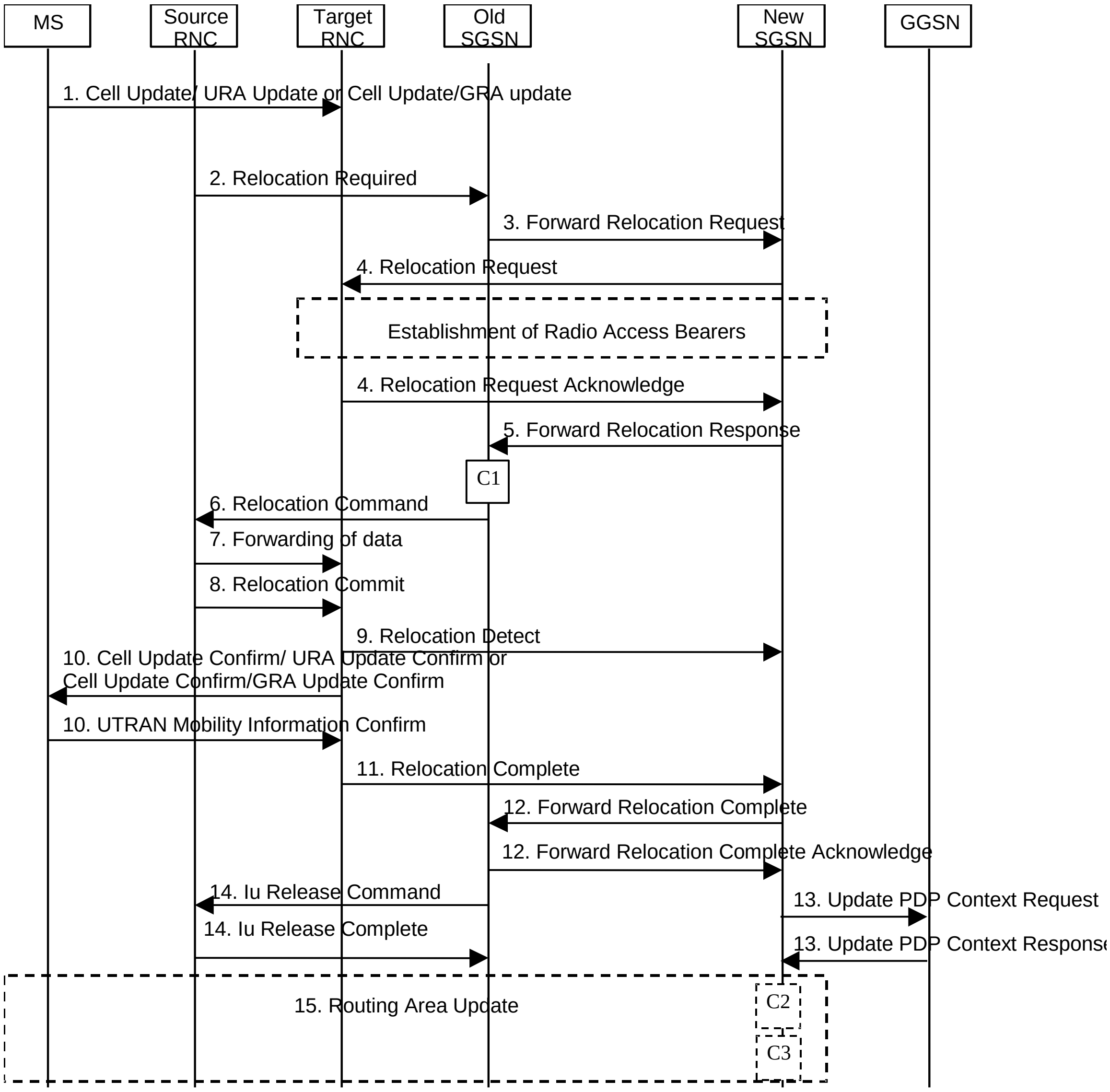
MS
Source RNC
Target RNC
Old SGSN
New SGSN
GGSN
1. Cell Update/ URA Update or Cell Update/GRA update
2. Relocation Required
3. Forward Relocation Request
4. Relocation Request
Establishment of Radio Access Bearers
4. Relocation Request Acknowledge
5. Forward Relocation Response
C1
6. Relocation Command
7. Forwarding of data
8. Relocation Commit
9. Relocation Detect
10. Cell Update Confirm/ URA Update Confirm or Cell Update Confirm/GRA Update Confirm
10. UTRAN Mobility Information Confirm
11. Relocation Complete
12. Forward Relocation Complete
12. Forward Relocation Complete Acknowledge
14. Iu Release Command
13. Update PDP Context Request
14. Iu Release Complete
13. Update PDP Context Response
15. Routing Area Update
C2
C3

Figure 6.9: Combined Cell/URA Update and SRNS Relocation Procedure

1) The MS sends a Cell Update / URA Update or a Cell Update / GRA Update message to the source SRNC (if the cell is located under another RNC the message is routed via the DRNC to SRNC over the Iur). The source SRNC decides whether or not to perform a combined cell / URA update and SRNS relocation towards the target RNC. The rest of this subclause describes the case where a combined cell / URA update and SRNS relocation applies. In this case no radio bearer is established between the source SRNC and the UE. Nonetheless the following tunnel(s) are established: GTP-U tunnel(s) between source SRNC and old-SGSN; GTP-U tunnel(s) between old-SGSN and GGSN.

2) The source SRNC sends a Relocation Required message (Relocation Type, Cause, Source ID, Target ID, Source RNC to Target RNC Transparent Container) to the old SGSN. The source SRNC shall set Relocation Type to "UE not involved". Source RNC to Target RNC Transparent Container includes the necessary information for Relocation co-ordination, security functionality, and RRC protocol context information (including MS Capabilities).

3) The old SGSN determines from the Target ID if the SRNS Relocation is intra-SGSN SRNS relocation or inter-SGSN SRNS relocation. In the case of inter-SGSN SRNS relocation the old SGSN initiates the relocation resource allocation procedure by sending a Forward Relocation Request (IMSI, Tunnel Endpoint Identifier

Signalling, MM Context, PDP Context, Target Identification, RAN Transparent Container, RANAP Cause) message to the new SGSN. For relocation to an area where Intra Domain Connection of RAN Nodes to Multiple CN Nodes is used, the old SGSN may – if it provides Intra Domain Connection of RAN Nodes to Multiple CN Nodes -have multiple target SGSNs for each relocation target in a pool area, in which case the old SGSN will select one of them to become the new SGSN, as specified in TS 23.236. PDP context contains GGSN Address for User Plane and Uplink TEID for Data (to this GGSN Address and Uplink TEID for Data, the old SGSN and the new SGSN send uplink packets). At the same time a timer is started on the MM and PDP contexts in the old SGSN, see Routeing Area Update procedure in subclause "Location Management Procedures (Iu mode)". The Forward Relocation Request message is applicable only in case of inter-SGSN SRNS relocation.

4) The new SGSN sends a Relocation Request message (Permanent NAS UE Identity, Cause, CN Domain Indicator, Source RNC to Target RNC Transparent Container, RABs To Be Setup) to the target RNC. For each requested RAB, RABs To Be Setup shall contain information such as RAB ID, RAB parameters, Transport Layer Address, and Iu Transport Association. SGSN shall not establish RABs for PDP contexts with maximum bitrate for uplink and downlink of 0 kbit/s. The RAB ID information element contains the NSAPI value, and the RAB parameters information element gives the QoS profile. The Transport Layer Address is the SGSN Address for user data, and the Iu Transport Association corresponds to the uplink Tunnel Endpoint Identifier Data.

   After all necessary resources for accepted RABs including the Iu user plane are successfully allocated, the target RNC shall send the Relocation Request Acknowledge message (RABs setup, RABs failed to setup) to the new SGSN. Each RAB to be setup is defined by a Transport Layer Address, which is the target RNC Address for user data, and a Iu Transport Association which corresponds to the downlink Tunnel Endpoint Identifier for user data.

   After the new SGSN receives the Relocation Request Acknowledge message, the GTP-U tunnels are established between the target RNC and the new-SGSN.

   The target-RNC may simultaneously receive for each RAB to be set up downlink user packets both from the source SRNC and from the new SGSN.

5) When resources for the transmission of user data between the target RNC and the new SGSN have been allocated and the new SGSN is ready for relocation of SRNS, the Forward Relocation Response message (Cause, RANAP Cause, and Target RNC Information) is sent from the new SGSN to the old SGSN. This message indicates that the target RNC is ready to receive from the source SRNC the forwarded downlink packets, i.e., the relocation resource allocation procedure is terminated successfully. RANAP Cause is information from the target RNC to be forwarded to the source SRNC. The RAB Setup Information, one information element for each RAB, contains the RNC Tunnel Endpoint Identifier and RNC IP address for data forwarding from the source SRNC to the target RNC. If the target RNC or the new SGSN failed to allocate resources, the RAB Setup Information element contains only NSAPI indicating that the source SRNC shall release the resources associated with the NSAPI. PDP contexts for emergency use (i.e. PDP context(s) with a globally dedicated emergency APN) shall have a high priority and therefore RABs for PDP contexts for emergency use should not be dropped in the SGSN during SRNS relocation procedure. The Forward Relocation Response message is applicable only in case of inter-SGSN SRNS relocation.

6) The old SGSN continues the relocation of SRNS by sending a Relocation Command (RABs to be released, and RABs subject to data forwarding) message to the source SRNC. The old SGSN decides the RABs subject to data forwarding based on QoS, and those RABs shall be contained in RABs subject to data forwarding. For each RAB subject to data forwarding, the information element shall contain RAB ID, Transport Layer Address, and Iu Transport Association. These are the same Transport Layer Address and Iu Transport Association that the target RNC had sent to new SGSN in Relocation Request Acknowledge message, and these are used for forwarding of downlink N-PDU from the source SRNC to the target RNC. The source SRNC is now ready to forward downlink data directly to the target RNC over the Iu interface. This forwarding is performed for downlink user data only.

7) The source SRNC may, according to the QoS profile, begin the forwarding of data for the RABs subject to data forwarding and starts the data-forwarding timer. The data forwarding at SRNS relocation shall be carried out through the Iu interface, meaning that the data exchanged between the source SRNC and the target RNC are duplicated in the source SRNC and routed at the IP layer towards the target RNC. For each radio bearer which uses lossless PDCP the GTP-PDUs related to transmitted but not yet acknowledged PDCP-PDUs are duplicated and routed at IP layer towards the target RNC together with their related downlink PDCP sequence numbers. The source RNC continues transmitting duplicates of downlink data and receiving uplink data.

NOTE: The order of steps, starting from step 7 onwards, does not necessarily reflect the order of events. For instance, source RNC may send data forwarding (step 7) and start Relocation Commit message (step 8) almost simultaneously. Target RNC may send Relocation Detect message (step 9) and Cell Update Confirm/URA Update Confirm (or Cell Update Confirm/GRA Update Confirm) message (step 10) at the same time. Hence, target RNC may receive the UTRAN or GERAN Mobility Information Confirm message from MS (step 10) while data forwarding (step 8) is still underway, and before the new SGSN receives Update PDP Context Response message (step 11).

Before the serving RNC role is not yet taken over by target RNC and when downlink user plane data starts to arrive to target RNC, the target RNC may buffer or discard arriving downlink GTP-PDUs according to the related QoS profile.

8) Before sending the Relocation Commit the uplink and downlink data transfer in the source, SRNC shall be suspended for RABs, which require delivery order.

When the source SRNC is ready, the source SRNC shall trigger the execution of relocation of SRNS by sending a Relocation Commit message (SRNS Contexts) to the target RNC over the UTRAN Iur interface or over the GERAN Iur-g interface, respectively. The purpose of this procedure is to transfer SRNS contexts from the source RNC to the target RNC, and to move the SRNS role from the source RNC to the target RNC. SRNS contexts are sent for each concerned RAB and contain the sequence numbers of the GTP-PDUs next to be transmitted in the uplink and downlink directions and the next PDCP sequence numbers that would have been used to send and receive data from the MS. . PDCP sequence numbers are only sent by the source RNC for radio bearers, which used lossless PDCP [57]. The use of lossless PDCP is selected by the RNC when the radio bearer is set up or reconfigured. For PDP context(s) using delivery order not required (QoS profile), the sequence numbers of the GTP-PDUs next to be transmitted are not used by the target RNC.

If delivery order is required (QoS profile), consecutive GTP-PDU sequence numbering shall be maintained throughout the lifetime of the PDP context(s). Therefore, during the entire SRNS relocation procedure for the PDP context(s) using delivery order required (QoS profile), the responsible GTP-U entities (RNCs and GGSN) shall assign consecutive GTP-PDU sequence numbers to user packets belonging to the same PDP context for uplink and downlink respectively.

9) The target RNC shall send a Relocation Detect message to the new SGSN when the relocation execution trigger is received. For SRNS relocation type "UE not involved", the relocation execution trigger is the reception of the Relocation Commit message from the Iur interface. When the Relocation Detect message is sent, the target RNC shall start SRNC operation.

10) The target SRNC sends a Cell Update Confirm / URA Update Confirm or Cell Update Confirm / GRA Update Confirm message. This message contains UE information elements and CN information elements. The UE information elements include among others new SRNC identity and S-RNTI. The CN information elements contain among others Location Area Identification and Routeing Area Identification. The procedure shall be co-ordinated in all Iu signalling connections existing for the MS.

Upon reception of the Cell Update Confirm / URA Update Confirm or Cell Update Confirm / GRA Update Confirm message the MS may start sending uplink user data to the target SRNC. When the MS has reconfigured itself, it sends the RAN Mobility Information Confirm message to the target SRNC. This indicates that the MS is also ready to receive downlink data from the target SRNC.

If the new SGSN has already received the Update PDP Context Response message from the GGSN, it shall forward the uplink user data to the GGSN over this new GTP-U tunnel. Otherwise, the new SGSN shall forward the uplink user data to that GGSN IP address and TEID(s), which the new SGSN had received earlier by the Forward Relocation Request message.

The target SRNC and the MS exchange the PDCP sequence numbers; PDCP-SNU and PDCP-SND. PDCP-SND is the PDCP sequence number for the next expected in-sequence downlink packet to be received in the MS per radio bearer, which used lossless PDCP in the source RNC. PDCP-SND confirms all mobile terminated packets successfully transferred before the SRNC relocation procedure. . If PDCP-SND confirms the reception of packets that were forwarded from the source SRNC, the target SRNC shall discard these packets. PDCP-SNU is the PDCP sequence number for the next expected in-sequence uplink packet to be received in the RNC per radio bearer, which used lossless PDCP in the source RNC. PDCP-SNU confirms all mobile originated packets successfully transferred before the SRNC relocation. If PDCP-SNU confirms reception of packets that were received in the source SRNC, the target SRNC shall discard these packets.

11) When the target SRNC receives the RAN Mobility Information Confirm message, i.e. the new SRNC-ID + S-RNTI are successfully exchanged with the MS by the radio protocols, the target SRNC shall initiate the Relocation Complete procedure by sending the Relocation Complete message to the new SGSN. The purpose of the Relocation Complete procedure is to indicate by the target SRNC the completion of the relocation of the SRNS to the CN.

12) Upon receipt of Relocation Complete message, if the SRNS Relocation is an inter SGSN SRNS relocation, the new SGSN signals to the old SGSN the completion of the SRNS relocation procedure by sending a Forward Relocation Complete message.

13) Upon receipt of the Relocation Complete message, the CN shall switch the user plane from the source RNC to the target SRNC. If the SRNS Relocation is an inter-SGSN SRNS relocation, the new SGSN sends Update PDP Context Request messages (new SGSN Address, SGSN Tunnel Endpoint Identifier, QoS Negotiated, serving network identity, CGI/SAI, RAT type) to the GGSNs concerned. The SGSN shall send the serving network identity to the GGSN. The GGSNs update their PDP context fields and return an Update PDP Context Response (GGSN Tunnel Endpoint Identifier, Prohibit Payload Compression, APN Restriction) message. The Prohibit Payload Compression indicates that the SGSN should negotiate no data compression for this PDP context.

14) Upon receiving the Relocation Complete message or if it is an inter-SGSN SRNS relocation, the Forward Relocation Complete message, the old SGSN sends an Iu Release Command message to the source RNC. When the RNC data-forwarding timer has expired the source RNC responds with an Iu Release Complete.

15) After the MS has finished the Cell / URA update or the Cell / GRA update and RNTI reallocation procedure and if the new Routeing Area Identification is different from the old one, the MS initiates the Routeing Area Update procedure. See subclause "Location Management Procedures (Iu mode)". Note that it is only a subset of the RA update procedure that is performed, since the MS is in PMM-CONNECTED state.

If the SRNS Relocation is inter-SGSN, then the following CAMEL procedure calls shall be performed (see referenced procedures in TS 23.078)

C1) CAMEL_GPRS_PDP_Context_Disconnection, CAMEL_GPRS_Detach and CAMEL_PS_Notification.

They are called in the following order:

- The CAMEL_GPRS_PDP_Context_Disconnection procedure is called several times: once per PDP context. The procedure returns as result "Continue".

- Then the CAMEL_GPRS_Detach procedure is called once. The procedure returns as result "Continue".

- Then the CAMEL_PS_Notification procedure is called once. The procedure returns as result "Continue".

The new SGSN shall determine the Maximum APN restriction based on the received APN Restriction of each PDP context from the GGSN and then store the new Maximum APN restriction value.

If the SRNS Relocation is intra-SGSN, then the above mentioned CAMEL procedures calls shall not be performed.

If Routeing Area Update occurs, then the following CAMEL procedure calls shall be performed (see referenced procedures in TS 23.078):

C2) CAMEL_GPRS_Routeing_Area_Update_Session and CAMEL_PS_Notification.

They are called in the following order:

- The CAMEL_GPRS_Routeing_Area_Update_Session procedure is called. The procedure returns as result "Continue".

- Then, the CAMEL_PS_Notification procedure is called. The procedure returns as result "Continue".

C3) CAMEL_GPRS_Routeing_Area_Update_Context.

This procedure is called several times: once per PDP context. It returns as result "Continue" . For C2 and C3: refer to Routing Area Update procedure description for detailed message flow.

NOTE: It is FFS whether CAMEL procedures are performed if the MS is emergency attached or if the MS has active PDP context(s) for an emergency use.

6.2.5 Service Request Procedure (Iu mode)

The Service Request procedure is used by a 3G-MS in PMM-IDLE state to request the establishment of a secure connection to a 3G-SGSN. The MS in PMM-IDLE state initiates this procedure in order to send uplink signalling messages (e.g. Activate PDP Context Request), user data, or as paging response, or after the MS has regained radio coverage. This procedure is also used by an MS in PMM-CONNECTED state to request resource reservation for active PDP contexts.

If the service request procedure is initiated for emergency use, the MS shall provide an emergency indication to the network. This indication informs the network that upcoming uplink signalling messages from the MS will be related to an emergency use and that special treatment may need to be applied.

In the context of this specification, the terms RNC refer also to a GERAN BSC when serving an MS in Iu mode.

6.2.5.1 MS Initiated Service Request Procedure

The MS in PMM-IDLE state sends the Service Request message to the 3G-SGSN in order to establish the PS signalling connection for the upper layer signalling or for the resource reservation for active PDP context(s). After receiving the Service Request message, the 3G-SGSN may perform authentication, and it shall perform the security mode procedure. After the establishment of the secure PS signalling connection to a 3G-SGSN, the MS may send signalling messages, e.g. Activate PDP Context Request, to the 3G-SGSN, or the 3G-SGSN may start the resource reservation for the active PDP contexts depending on the requested service in the Service Request message. An MS in PMM-CONNECTED state also requests the resource reservation for the active PDP contexts through this procedure.

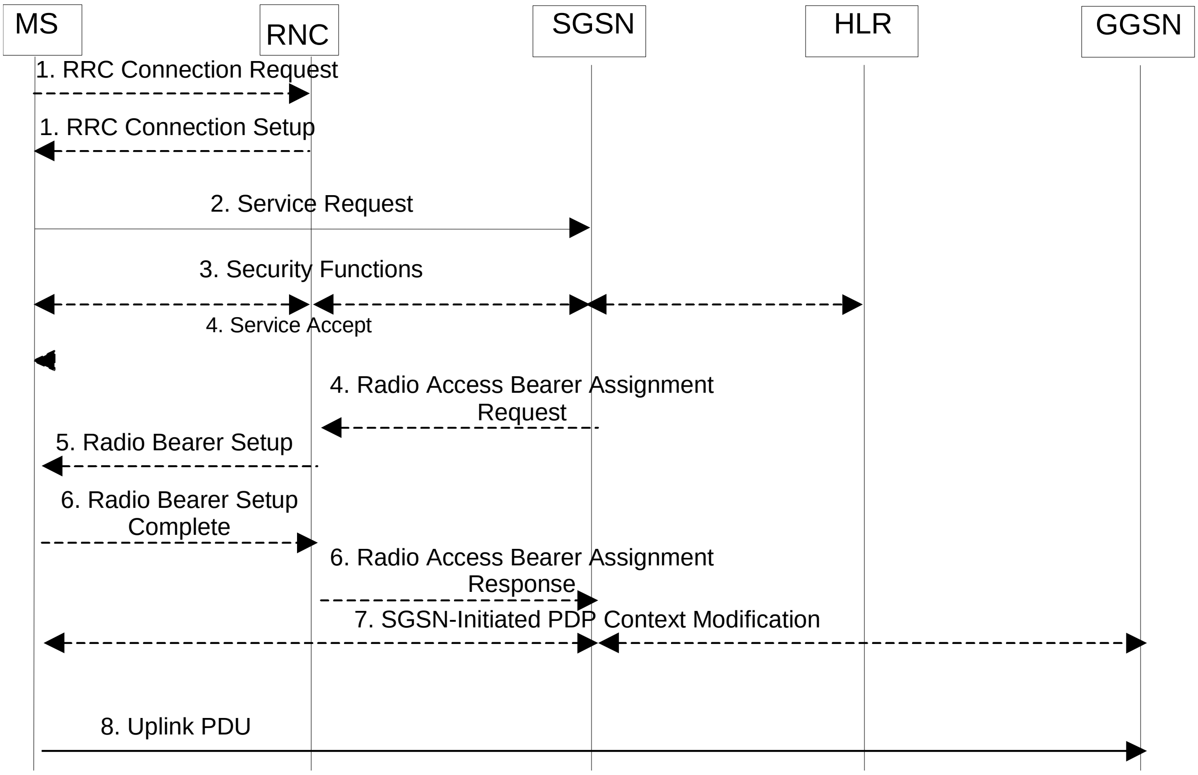
MS
RNC
SGSN
HLR
GGSN
1. RRC Connection Request
1. RRC Connection Setup
2. Service Request
3. Security Functions
4. Service Accept
4. Radio Access Bearer Assignment Request
5. Radio Bearer Setup
6. Radio Bearer Setup Complete
6. Radio Access Bearer Assignment Response
7. SGSN-Initiated PDP Context Modification
8. Uplink PDU

Figure 6.10: MS Initiated Service Request Procedure

1) The MS establishes an RRC connection, if none exists for CS traffic.

2) The MS sends a Service Request (P-TMSI, RAI, CKSN, Service Type, Emergency Indication) message to the SGSN. Service Type specifies the requested service. Service Type shall indicate one of the following: Data or Signalling. At this point, the SGSN may perform the authentication procedure.

   If Service Type indicates Data, a signalling connection is established between the MS and the SGSN, and resources for active PDP context(s) are allocated, i.e. RAB establishment for the activated PDP context(s).

If Service Type indicates Signalling, the signalling connection is established between the MS and the SGSN for sending upper-layer signalling messages, e.g. Activate PDP Context Request. The resources for active PDP context(s) are not allocated.

The MS shall use the Emergency Indication to signal whether the Service Request is for emergency use.

3) The SGSN shall perform the security functions if the MS in PMM-IDLE state initiated the service request.

4) If the network is in PMM-CONNECTED state and the Service Type indicates Data, the SGSN shall respond with a Service Accept message towards the MS, in case the service request can be accepted. In case Service Type indicates Data, the SGSN sends a Radio Access Bearer Assignment Request (NSAPIRAB ID(s), TEID(s), QoS Profile(s), SGSN IP Address(es)) message to re-establish radio access bearer for every activated PDP context, except the ones having maximum bit rates for uplink and downlink of 0 kbit/s.

5) The RNC indicates to the MS the new Radio Bearer Identity established and the corresponding RAB ID with the RRC radio bearer setup procedure.

6) SRNC responds with the Radio Access Bearer Assignment Response (RAB ID(s), TEID(s), QoS Profile(s), RNC IP Address(es)) message. The GTP tunnel(s) are established on the Iu interface. If the RNC returns a Radio Access Bearer Assignment Response message with a cause indicating that the requested QoS profile(s) can not be provided, e.g. "Requested Maximum Bit Rate not Available", the SGSN may send a new Radio Access Bearer Assignment Request message with different QoS profile(s). The number of re-attempts, if any, as well as how the new QoS profile(s) values are determined is implementation dependent.

7) For each RAB re-established with a modified QoS profile, the SGSN initiates a PDP Context Modification procedure to inform the MS and the GGSN of the new negotiated QoS profile for the corresponding PDP context.

8) The MS sends the uplink packet.

For Service Type = Signalling, the MS knows that the Service Request message was successfully received in the SGSN when the MS receives the RRC Security Mode Control Command message.

For Service Type = Data, in PMM-IDLE, the MS knows that the Service Request was successfully received when the MS receives the RRC Security Mode Control Command message from the RNC; in PMM-CONNECTED state, the MS knows that the Service Request was successfully received when the MS receives the Service Accept message.

NOTE: The reception of the Service Accept message does not imply the successful re-establishment of the RAB(s).

For any Service Type, in case the service request cannot be accepted, the network returns a Service Reject message to the MS with an appropriate cause value.

For Service Type = Data, in case the SGSN fails to re-establish RAB(s) for the PDP context(s), the SGSN determines if an SM procedure, such as SGSN-Initiated PDP Context Modification or PDP Context Deactivation, should be initiated. The appropriate action depends on the QoS profile of the PDP context and is an operator choice.

If in PMM-CONNECTED state, a Service Request with Service Type = Data was already accepted by the network the MS shall not issue a second Service Request with Service Type = Data unless the PMM-IDLE state is entered again.

For each PDP context using streaming or conversational traffic class with maximum bit rate for uplink and downlink of 0 kbit/s the MS starts the MS-Initiated PDP Context Modification procedure or the MS-Initiated PDP Context Deactivation procedure to inform the SGSN whether to re-activate or to delete the PDP contexts. If the PDP context has been deactivated locally in the MS, the MS shall not perform the PDP context deactivation procedure for this PDP context because the list of active and inactive PDP contexts is included in the Service Request Message sent prior to the network.

6.2.6 Intersystem Change

6.2.6.1 Iu mode to A/Gb mode Inter-SGSN Change

An inter-SGSN inter-system change from Iu mode to A/Gb mode takes place when an MS in PMM-IDLE or PMM-CONNECTED state changes from UTRAN or GERAN Iu mode to A/Gb mode and the A/Gb mode radio access node serving the MS is served by a different SGSN. In this case, the RA changes. Therefore, the MS shall initiate a A/Gb mode RA update procedure. The RA update procedure is either combined RA/LA update or only RA update. These RA update cases are illustrated in Figure 6.11. In the context of this specification, the terms RNS or RNC refer also to a GERAN BSS or BSC (respectively) when serving an MS in Iu mode.

A combined RA/LA update takes place in network operation mode I when the MS enters a new RA or when a GPRS-attached MS performs IMSI attach. The MS sends a Routeing Area Update Request indicating that an LA update may also need to be performed, in which case the SGSN forwards the LA update to the VLR. This concerns only idle mode (see TS 23.122), as no combined RA/LA updates are performed during a CS connection.

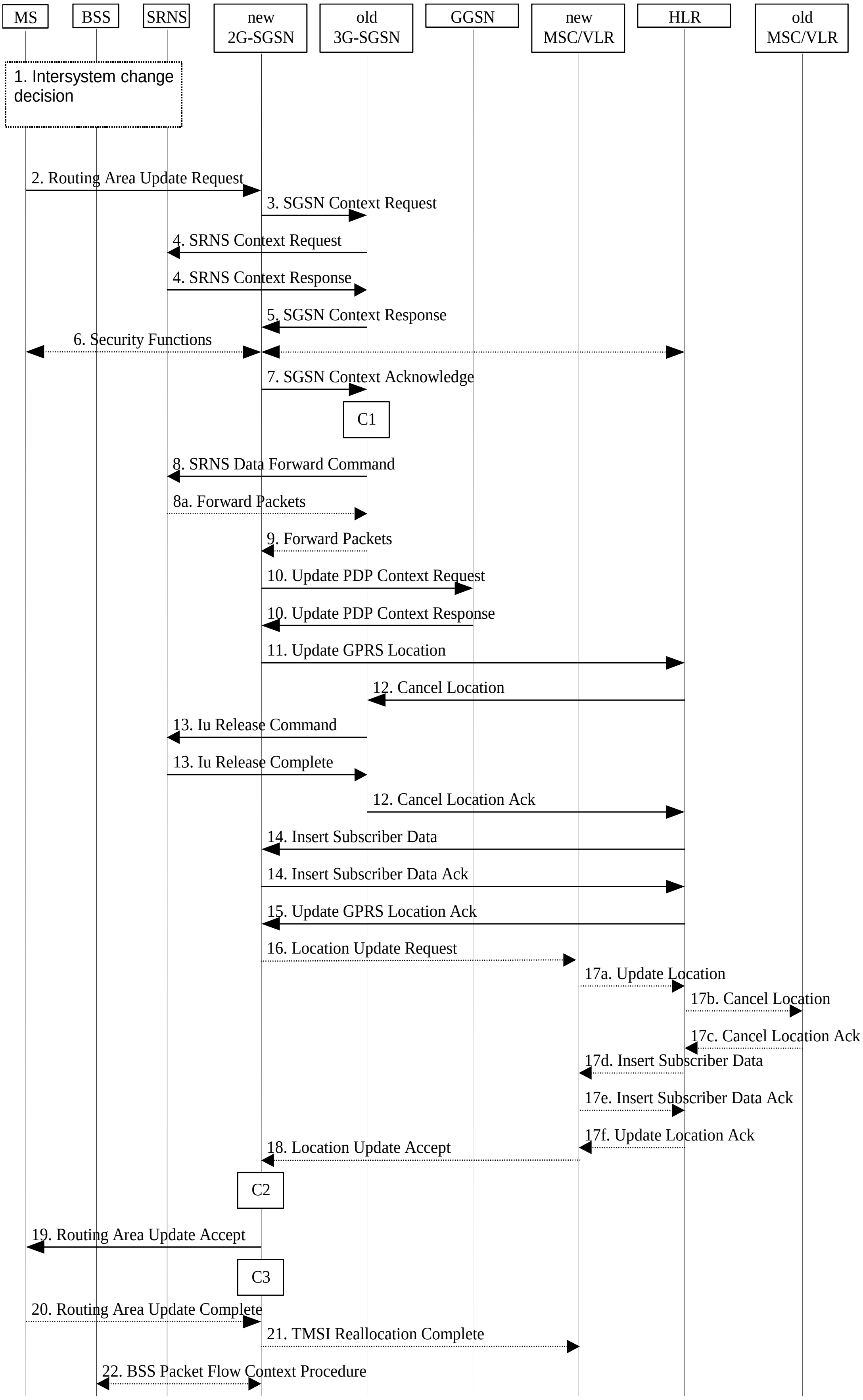
MS
BSS
SRNS
new 2G-SGSN
old 3G-SGSN
GGSN
new MSC/VLR
HLR
old MSC/VLR
1. Intersystem change decision
2. Routing Area Update Request
3. SGSN Context Request
4. SRNS Context Request
4. SRNS Context Response
5. SGSN Context Response
6. Security Functions
7. SGSN Context Acknowledge
C1
8. SRNS Data Forward Command
8a. Forward Packets
9. Forward Packets
10. Update PDP Context Request
10. Update PDP Context Response
11. Update GPRS Location
12. Cancel Location
13. Iu Release Command
13. Iu Release Complete
12. Cancel Location Ack
14. Insert Subscriber Data
14. Insert Subscriber Data Ack
15. Update GPRS Location Ack
16. Location Update Request
17a. Update Location
17b. Cancel Location
17c. Cancel Location Ack
17d. Insert Subscriber Data
17e. Insert Subscriber Data Ack
17f. Update Location Ack
18. Location Update Accept
C2
19. Routing Area Update Accept
C3
20. Routing Area Update Complete
21. TMSI Reallocation Complete
22. BSS Packet Flow Context Procedure

Figure 6.11: Iu mode to A/Gb mode Inter-SGSN Change

1) The MS or RAN decides to perform an inter-system change, which makes the MS switch to a new cell where A/Gb mode has to be used, and stops transmission to the network.

2) The MS sends a Routeing Area Update Request (old RAI, old P-TMSI Signature, Update Type, MS Network Capability) message to the new 2G-SGSN. Update Type shall indicate RA update or combined RA/LA update, or, if the MS wants to perform an IMSI attach, combined RA/LA update with IMSI attach requested. The BSS shall add the Cell Global Identity including the RAC and LAC of the cell where the message was received before passing the message to the new 2G-SGSN.

3) The new 2G-SGSN sends an SGSN Context Request (old RAI, TLLI, old P-TMSI Signature, New SGSN Address) message to the old 3G-SGSN to get the MM and PDP contexts for the MS. If the new SGSN provides functionality for Intra Domain Connection of RAN Nodes to Multiple CN Nodes, the new SGSN may derive the old SGSN from the old RAI and the old P-TMSI (or TLLI) and send the SGSN Context Request message to this old SGSN. Otherwise, the new SGSN derives the old SGSN from the old RAI. In any case the new SGSN will derive an SGSN that it believes is the old SGSN. This derived SGSN is itself the old SGSN, or it is associated with the same pool area as the actual old SGSN and it will determine the correct old SGSN from the P-TMSI (or TLLI) and relay the message to that actual old SGSN. The old 3G-SGSN validates the old P-TMSI Signature and responds with an appropriate error cause if it does not match the value stored in the old 3G-SGSN. If the received old P-TMSI Signature does not match the stored value, the security functions in the new 2G-SGSN should be initiated. If the security functions authenticate the MS correctly, the new 2G-SGSN shall send an SGSN Context Request (old RAI, TLLI, MS Validated, New SGSN Address) message to the old 3G-SGSN. MS Validated indicates that the new 2G-SGSN has authenticated the MS. If the old P-TMSI Signature was valid or if the new 2G-SGSN indicates that it has authenticated the MS correctly, the old 3G-SGSN starts a timer. If the MS is not known in the old 3G-SGSN, the old 3G-SGSN responds with an appropriate error cause.

4) If the MS is PMM-CONNECTED the old 3G-SGSN sends an SRNS Context Request (IMSI) message to the SRNS. Upon receipt of this message the SRNS buffers and stops sending downlink PDUs to the MS and returns an SRNS Context Response (GTP-SNDs, GTP-SNUs, PDCP-SNDs, PDCP-SNUs) message. The SRNS shall include for each PDP context the next in-sequence GTP sequence number to be sent to the MS and the GTP sequence number of the next uplink PDU to be tunnelled to the GGSN. For each active PDP context, which uses lossless PDCP, the SRNS also includes the uplink PDCP sequence number (PDCP-SNU) downlink PDCP sequence number (PDCP-SND). PDCP-SNU shall be the next in-sequence PDCP sequence number expected from the MS. PDCP-SND is the PDCP sequence number for the first downlink packet for which successful transmission has not been confirmed. The 3G-SGSN shall strip off the eight most significant bits of the passed PDCP sequence numbers, thus converting them to SNDCP N-PDU numbers and stores the N-PDU numbers in its PDP contexts.

5) The old 3G-SGSN responds with an SGSN Context Response (MM Context, PDP Contexts) message. For each PDP context the old 3G-SGSN shall include the GTP sequence number for the next uplink GTP PDU to be tunnelled to the GGSN and the next downlink GTP sequence number for the next in-sequence N-PDU to be sent to the MS. Each PDP Context also includes the SNDCP Send N-PDU Number (the value is 0) for the next in-sequence downlink N-PDU to be sent in SNDCP acknowledged mode to the MS and the SNDCP Receive N-PDU Number (= converted PDCP-SNU) for the next in-sequence uplink N-PDU to be received in SNDCP acknowledged mode from the MS. The new 3G-SGSN shall ignore the MS Network Capability contained in MM Context of SGSN Context Response only when it has previously received an MS Network Capability in the Routeing Area Request.

6) Security functions may be executed.

7) The new 2G-SGSN sends an SGSN Context Acknowledge message to the old 3G-SGSN. This informs the old 3G-SGSN that the new 2G-SGSN is ready to receive data packets belonging to the activated PDP contexts. The old SGSN marks in its context that the MSC/VLR association and the information in the GGSNs and the HLR are invalid. This triggers the MSC/VLR, the GGSNs, and the HLR to be updated if the MS initiates a RA update procedure back to the old SGSN before completing the ongoing RA update procedure.

8) If the MS is in the PMM-CONNECTED state, the old 3G-SGSN sends an SRNS Data Forward Command (RAB ID, Transport Layer Address, Iu Transport Association) message to the SRNS. For each indicated RAB the SRNS starts duplicating and tunnelling the buffered GTP PDUs to the old 3G-SGSN. For each radio bearer which uses lossless PDCP the SRNS shall start tunnelling the GTP-PDUs related to transmitted but not yet acknowledged PDCP-PDUs to the old 3G-SGSN together with their related downlink PDCP sequence numbers. Upon receipt of the SRNS Data Forward Command message from the 3G-SGSN, the SRNS shall start the data-forwarding timer.

9) The old 3G-SGSN tunnels the GTP PDUs to the new 2G-SGSN. In the case of GTPv1, the conversion of PDCP sequence numbers to SNDCP sequence numbers (the eight most significant bits shall be stripped off) shall be done in the new SGSN. No N-PDU sequence numbers shall be indicated for these N-PDUs. If GTPv0 is used

between the SGSNs, the conversion of PDCP sequence numbers to SNDCP numbers shall be done in the old 3G-SGSN (by stripping off the eight most significant bits).

10) The new 2G-SGSN sends an Update PDP Context Request (new SGSN Address, TEID, QoS Negotiated) message to each GGSN concerned. Each GGSN updates its PDP context fields and returns an Update PDP Context Response (TEID) message.

11) The new 2G-SGSN informs the HLR of the change of SGSN by sending an Update GPRS Location (SGSN Number, SGSN Address, IMSI) message to the HLR.

12) The HLR sends a Cancel Location (IMSI) message to the old 3G-SGSN. The old 3G-SGSN acknowledges with a Cancel Location Ack (IMSI) message. The old 3G-SGSN removes the MM and PDP contexts if the timer described in step 3 is not running. If the timer is running, the MM and PDP contexts shall be removed when the timer expires.

13) When the MS is PMM-CONNECTED, the old 3G-SGSN sends an Iu Release Command message to the SRNS. When the RNC data-forwarding timer has expired, the SRNS responds with an Iu Release Complete message.

14) The HLR sends an Insert Subscriber Data (IMSI, GPRS Subscription Data) message to the new 2G-SGSN. The 2G-SGSN constructs an MM context and PDP contexts for the MS and returns an Insert Subscriber Data Ack (IMSI) message to the HLR.

15) The HLR acknowledges the Update GPRS Location by returning an Update GPRS Location Ack (IMSI) message to the new 2G-SGSN.

16) If the association has to be established i.e. if Update Type indicates combined RA/LA update with IMSI attach requested, or if the LA changed with the routeing area update, the new 2G-SGSN sends a Location Update Request (new LAI, IMSI, SGSN Number, Location Update Type) to the VLR. Location Update Type shall indicate IMSI attach if Update Type in step 1 indicated combined RA/LA update with IMSI attach requested. Otherwise, Location Update Type shall indicate normal location update. When the SGSN does not provide functionality for the Intra Domain Connection of RAN Nodes to Multiple CN Nodes, the VLR number is derived from the RAI. When the SGSN provides functionality for Intra Domain Connection of RAN Nodes to Multiple CN Nodes, the SGSN uses the RAI and a hash value from the IMSI to determine the VLR number. The 2G-SGSN starts the location update procedure towards the new MSC/VLR upon receipt of the first Insert Subscriber Data message from the HLR in step 14). The VLR creates or updates the association with the 2G-SGSN by storing SGSN Number.

17) If the subscriber data in the VLR is marked as not confirmed by the HLR, the new VLR informs the HLR. The HLR cancels the old VLR and inserts subscriber data in the new VLR:

a) The new VLR sends an Update Location (new VLR) to the HLR.

b) The HLR cancels the data in the old VLR by sending Cancel Location (IMSI) to the old VLR.

c) The old VLR acknowledges with Cancel Location Ack (IMSI).

d) The HLR sends Insert Subscriber Data (IMSI, subscriber data) to the new VLR.

e) The new VLR acknowledges with Insert Subscriber Data Ack (IMSI).

f) The HLR responds with Update Location Ack (IMSI) to the new VLR.

18) The new VLR allocates a new TMSI and responds with Location Update Accept (VLR TMSI) to the 2G-SGSN. VLR TMSI is optional if the VLR has not changed.

19) The new 2G-SGSN validates the MS's presence in the new RA. If due to roaming restrictions the MS is not allowed to be attached in the RA, or if subscription checking fails, the new 2G-SGSN rejects the routeing area update with an appropriate cause. If the MS is emergency attached or if the MS has active PDP context(s) for an emergency use, the SGSN should not reject the routing area update due to e.g. roaming restrictions. If all checks are successful, the new 2G-SGSN constructs MM and PDP contexts for the MS. A logical link is established between the new 2G-SGSN and the MS. 2G-SGSN initiates the establishment procedure. The new 2G-SGSN responds to the MS with a Routeing Area Update Accept (P-TMSI, P-TMSI Signature, Receive N-PDU Number (= converted PDCP-SNU) message. Receive N-PDU Number contains the acknowledgements for each NSAPI which used lossless PDCP before the start of the update procedure, thereby confirming all mobile-originated

N-PDUs successfully transferred before the start of the update procedure. If Receive N-PDU Number confirms the reception of N-PDUs, the MS shall discard these N-PDUs.

20) The MS acknowledges the new P-TMSI by returning a Routeing Area Update Complete (Receive N-PDU Number (= converted PDCP-SND)) message to the SGSN. Receive N-PDU Number contains the acknowledgements for each lossless PDCP used by the MS before the start of the update procedure, thereby confirming all mobile-terminated N-PDUs successfully transferred before the start of the update procedure. If Receive N-PDU Number confirms the reception of N-PDUs that were forwarded from the old 3G-SGSN, the new 2G-SGSN shall discard these N-PDUs. The MS deducts Receive N-PDU number from PDCP-SND by stripping off the eight most significant bits. PDCP-SND is the PDCP sequence number for the next expected in-sequence downlink packet to be received in the MS per radio bearer, which used lossless PDCP. The new 2G-SGSN negotiates with the MS for each NSAPI the use of acknowledged or unacknowledged SNDCP regardless whether the SRNS used lossless PDCP or not.

21) The new 2G-SGSN sends TMSI Reallocation Complete message to the new VLR if the MS confirms the VLR TMSI.

22) The 2G-SGSN and the BSS may execute the BSS Packet Flow Context procedure.

If the new SGSN is unable to update the PDP context in one or more GGSNs, the new SGSN shall deactivate the corresponding PDP contexts as described in subclause "SGSN-initiated PDP Context Deactivation Procedure". This shall not cause the SGSN to reject the routeing area update.

The PDP Contexts shall be sent from old to new SGSN in a prioritized order, i.e. the most important PDP Context first in the SGSN Context Response message. (The prioritization method is implementation dependent, but should be based on the current activity.)

If the new SGSN is unable to support the same number of active PDP contexts as received from old SGSN, the new SGSN should use the prioritisation sent by old SGSN as input when deciding which PDP contexts to maintain active and which ones to delete. PDP contexts related to an emergency use shall have a high priority and therefore PDP contexts for emergency use should not be deactivated during the routeing area update. In any case, the new SGSN shall first update all contexts in one or more GGSNs and then deactivate the context(s) that it cannot maintain as described in subclause "SGSN-initiated PDP Context Deactivation Procedure". This shall not cause the SGSN to reject the routeing area update.

The CAMEL procedure calls shall be performed, see referenced procedures in TS 23.078:

C1) CAMEL_GPRS_PDP_Context_Disconnection, CAMEL_GPRS_Detach and CAMEL_PS_Notification.

They are called in the following order:

- The CAMEL_GPRS_PDP_Context_Disconnection procedure is called several times: once per PDP context. The procedure returns as result "Continue".
- Then the CAMEL_GPRS_Detach procedure is called once. The procedure returns as result "Continue".
- Then the CAMEL_PS_Notification procedure is called once. The procedure returns as result "Continue".

C2) CAMEL_GPRS_Routeing_Area_Update_Session and CAMEL_PS_Notification.

They are called in the following order:

- The CAMEL_GPRS_Routeing_Area_Update_Session procedure is called. The procedure returns as result "Continue".
- Then the CAMEL_PS_Notification procedure is called. The procedure returns as result "Continue".

C3) CAMEL_GPRS_Routeing_Area_Update_Context.

This procedure is called several times once per PDP context. It returns as result "Continue".

6.2.6.2 A/Gb mode to Iu mode Inter-SGSN Change

The inter-system change from A/Gb mode to Iu mode takes place when a GPRS-attached MS changes from A/Gb mode to UTRAN or GERAN Iu mode and the new RAN node serving the MS is served by a different SGSN. In this case the RA changes. Therefore, the MS shall initiate a Iu mode RA update procedure by establishing an RRC connection and initiating the RA update procedure. The RA update procedure is either combined RA/LA update or only RA update, these RA update cases are illustrated in figure 6.12. In the context of this specification, the terms RNS or RNC refer also to a GERAN BSS or BSC (respectively) when serving an MS in Iu mode.

If the network operates in mode I, then an MS, that is both PS-attached and CS-attached, shall perform the Combined RA/LA Update procedures. This concerns only idle mode (see TS 23.122), as no combined RA/LA updates are performed during a CS connection.

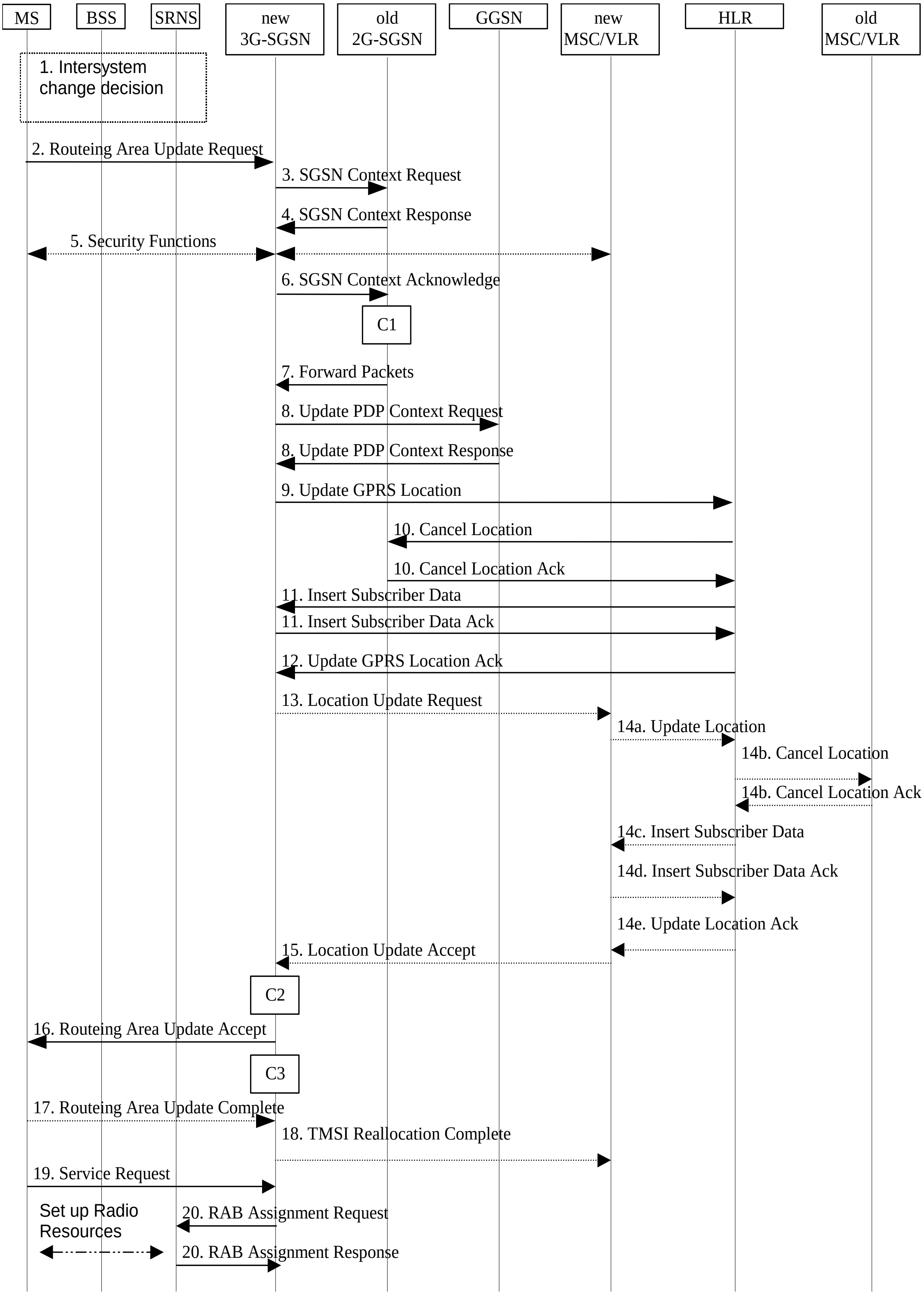
MS
BSS
SRNS
new 3G-SGSN
old 2G-SGSN
GGSN
new MSC/VLR
HLR
old MSC/VLR
1. Intersystem change decision
2. Routeing Area Update Request
3. SGSN Context Request
4. SGSN Context Response
5. Security Functions
6. SGSN Context Acknowledge
C1
7. Forward Packets
8. Update PDP Context Request
8. Update PDP Context Response
9. Update GPRS Location
10. Cancel Location
10. Cancel Location Ack
11. Insert Subscriber Data
11. Insert Subscriber Data Ack
12. Update GPRS Location Ack
13. Location Update Request
14a. Update Location
14b. Cancel Location
14b. Cancel Location Ack
14c. Insert Subscriber Data
14d. Insert Subscriber Data Ack
14e. Update Location Ack
15. Location Update Accept
C2
16. Routeing Area Update Accept
C3
17. Routeing Area Update Complete
18. TMSI Reallocation Complete
19. Service Request
Set up Radio Resources
20. RAB Assignment Request
20. RAB Assignment Response

Figure 6.12: A/Gb mode to Iu mode Inter SGSN Change

1) The MS or RAN decides to perform an inter-system change, which makes the MS switch to a new cell where Iu mode has to be used, and stops transmission to the network.

2) The MS sends a Routeing Area Update Request (P-TMSI, old RAI, old P-TMSI Signature, Update Type, CM, MS Network Capability) message to the new 3G-SGSN. Update Type shall indicate RA update or combined RA/LA update, or, if the MS wants to perform an IMSI attach, combined RA/LA update with IMSI attach requested, and also if the MS has a follow-on request, i.e. if there is pending uplink traffic (signalling or data). The SGSN may use, as an implementation option, the follow-on request indication to release or keep the Iu connection after the completion of the RA update procedure. The SRNC shall add the Routeing Area Identity including the RAC and LAC of the area where the MS is located before forwarding the message to the 3G-SGSN. This RA identity corresponds to the RAI in the MM system information sent by the SRNC to the MS.

3) The new 3G-SGSN uses the old RAI received from the MS to derive the old 2G-SGSN address, and sends an SGSN Context Request (old RAI, old P-TMSI, New SGSN Address) message to the old 2G-SGSN to get the MM and PDP contexts for the MS. If the new SGSN provides functionality for Intra Domain Connection of RAN Nodes to Multiple CN Nodes, the new SGSN may derive the old SGSN from the old RAI and the old P-TMSI and send the SGSN Context Request message to this old SGSN. Otherwise, the new SGSN derives the old SGSN from the old RAI. In any case the new SGSN will derive an SGSN that it believes is the old SGSN. This derived SGSN is itself the old SGSN, or it is associated with the same pool area as the actual old SGSN and it will determine the correct old SGSN from the P-TMSI and relay the message to that actual old SGSN. The old 2G-SGSN validates the old P-TMSI Signature and responds with an appropriate error cause if it does not match the value stored in the old 2G-SGSN. If the received old P-TMSI Signature does not match the stored value, the old 2G-SGSN should initiate the security functions in the new 3G-SGSN. If the security functions authenticate the MS correctly, the new 3G-SGSN shall send an SGSN Context Request (old RAI, IMSI, MS Validated, New SGSN Address) message to the old 2G-SGSN. MS Validated indicates that the new 3G-SGSN has authenticated the MS. If the old P-TMSI Signature was valid or if the new 3G-SGSN indicates that it has authenticated the MS correctly, the old 2G-SGSN starts a timer and stops the transmission of N-PDUs to the MS.

4) The old 2G-SGSN responds with an SGSN Context Response (MM Context, PDP Contexts) message. Each PDP Context includes the GTP sequence number for the next downlink N-PDU to be sent to the MS and the GTP sequence number for the next uplink N-PDU to be tunnelled to the GGSN. Each PDP Context also includes the SNDCP Send N-PDU Number for the next downlink N-PDU to be sent in acknowledged mode SNDCP to the MS and the SNDCP Receive N-PDU Number for the next uplink N-PDU to be received in acknowledged mode SNDCP from the MS. The new 3G-SGSN derives the corresponding PDCP sequence numbers from these N-PDU sequence numbers by adding eight most significant bits "1". These PDCP sequence numbers are stored in the 3G-SGSN PDP contexts. The new 3G-SGSN shall ignore the MS Network Capability contained in MM Context of SGSN Context Response only when it has previously received an MS Network Capability in the Routeing Area Request.

5) Security functions may be executed.

6) The new 3G-SGSN sends an SGSN Context Acknowledge message to the old 2G-SGSN. This informs the old 2G-SGSN that the new 3G-SGSN is ready to receive data packets belonging to the activated PDP contexts. The old SGSN marks in its context that the MSC/VLR association and the information in the GGSNs and the HLR are invalid. This triggers the MSC/VLR, the GGSNs, and the HLR to be updated if the MS initiates a routeing area update procedure back to the old SGSN before completing the ongoing routeing area update procedure.

7) The old 2G-SGSN duplicates the buffered N-PDUs and starts tunnelling them to the new 3G-SGSN. Additional N-PDUs received from the GGSN before the timer described in step 3 expires are also duplicated and tunnelled to the new 3G-SGSN. N-PDUs that were already sent to the MS in acknowledged mode SNDCP and that are not yet acknowledged by the MS are tunnelled together with their related SNDCP N-PDU sequence number. No PDCP sequence numbers shall be indicated for these N-PDUs. No N-PDUs shall be forwarded to the new 3G-SGSN after expiry of the timer described in step 3.

8) The new 3G-SGSN sends an Update PDP Context Request (new SGSN Address, TEID, QoS Negotiated) message to each GGSN concerned. Each GGSN updates its PDP context fields and returns an Update PDP Context Response (TEID) message.

9) The new 3G-SGSN informs the HLR of the change of SGSN by sending an Update GPRS Location (SGSN Number, SGSN Address, IMSI) message to the HLR.

10) The HLR sends a Cancel Location (IMSI, Cancellation Type) message to the old 2G-SGSN. The old 2G-SGSN removes the MM and PDP contexts if the timer described in step 3 is not running. If the timer is running, the MM and PDP contexts are removed when the timer expires. The old 2G-SGSN acknowledges with a Cancel Location Ack (IMSI) message.

11) The HLR sends an Insert Subscriber Data (IMSI, GPRS Subscription Data) message to the new 3G-SGSN. The 3G-SGSN constructs an MM context for the MS and returns an Insert Subscriber Data Ack (IMSI) message to the HLR.

12) The HLR acknowledges the Update GPRS Location by returning an Update GPRS Location Ack (IMSI) message to the new 3G-SGSN.

13) If the association has to be established, if Update Type indicates combined RA/LA update with IMSI attach requested, or if the LA changed with the routeing area update, the new SGSN sends a Location Update Request (new LAI, IMSI, SGSN Number, Location Update Type) to the VLR. Location Update Type shall indicate IMSI attach if Update Type in step 1 indicated combined RA/LA update with IMSI attach requested. Otherwise, Location Update Type shall indicate normal location update. When the SGSN does not provide functionality for the Intra Domain Connection of RAN Nodes to Multiple CN Nodes, the VLR number is derived from the RAI. When the SGSN provides functionality for Intra Domain Connection of RAN Nodes to Multiple CN Nodes, the SGSN uses the RAI and a hash value from the IMSI to determine the VLR number. The 3G-SGSN starts the location update procedure towards the new MSC/VLR upon receipt of the first Insert Subscriber Data message from the HLR in step 12). The VLR creates or updates the association with the 3G-SGSN by storing SGSN Number.

14) If the subscriber data in the VLR is marked as not confirmed by the HLR, the new VLR informs the HLR. The HLR cancels the old VLR and inserts subscriber data in the new VLR:

   a) The new VLR sends an Update Location (new VLR) to the HLR.

   b) The HLR cancels the data in the old VLR by sending Cancel Location (IMSI) to the old VLR.

   c) The old VLR acknowledges with Cancel Location Ack (IMSI).

   d) The HLR sends Insert Subscriber Data (IMSI, subscriber data) to the new VLR.

   e) The new VLR acknowledges with Insert Subscriber Data Ack (IMSI).

   f) The HLR responds with Update Location Ack (IMSI) to the new VLR.

15) The new VLR allocates a new TMSI and responds with Location Update Accept (VLR TMSI) to the 3G-SGSN. VLR TMSI is optional if the VLR has not changed.

16) The new 3G-SGSN validate the MS's presence in the new RA. If due to roaming restrictions the MS is not allowed to be attached in the RA, or if subscription checking fails, the new 3G-SGSN rejects the routeing area update with an appropriate cause. If the MS is emergency attached or if the MS has active PDP context(s) for an emergency use, the SGSN should not reject the routing area update due to e.g. roaming restrictions. If all checks are successful, the new 3G-SGSN constructs MM and PDP contexts for the MS. The new 3G-SGSN responds to the MS with a Routeing Area Update Accept (P-TMSI, P-TMSI signature) message.

17) The MS acknowledges the new P-TMSI by returning a Routeing Area Update Complete message to the SGSN.

18) The new 3G-SGSN sends TMSI Reallocation Complete message to the new VLR, if the MS confirms the VLR TMSI.

19) If the MS has uplink data or signalling pending it shall send a Service Request (P-TMSI, RAI, CKSN, Service Type) message to the SGSN. Service Type specifies the requested service. Service Type shall indicate one of the following: Data or Signalling.

20) If the MS has sent the Service Request, the new 3G-SGSN requests the SRNS to establish a radio access bearer by sending a RAB Assignment Request (RAB ID(s), QoS Profile(s), GTP-SNDs, GTP-SNUs, PDCP-SNUs) message to the SRNS. The PDCP sequence numbers are derived from the N-PDU sequence numbers in step 4) and stored in the SGSN PDP contexts. The SRNS sends a Radio Bearer Setup Request (PDCP-SNUs) message to the MS. The MS responds with a Radio Bearer Setup Complete (PDCP-SNDs) message. The MS deducts PDCP-SND from its Receive N-PDU Number by adding eight most significant bits "1". The SRNS responds with a RAB Assignment Response message. The SRNS shall discard all N-PDUs tunnelled from the SGSN with N-PDU sequence numbers older than the eight least significant bits of the PDCP-SNDs received from the MS. Other N-PDUs shall be transmitted to the MS. The MS shall discard all N-PDUs with SNDCP sequence numbers older than the eight least significant bits of the PDCP-SNUs received from the SRNS. Other N-PDUs shall be transmitted to the SRNS. The SRNS negotiates with the MS for each radio bearer the use of lossless PDCP or

not regardless whether the old 2G-SGSN used acknowledged or unacknowledged SNDCP for the related NSAPI or not.

NOTE 1: The NSAPI value is carried in the RAB ID IE.

NOTE 2: The new SGSN may initiate RAB establishment after execution of the security functions (step 5), or wait until completion of the RA update procedure. For the MS, RAB establishment may occur anytime after the RA update request is sent (step 2).

If the new SGSN is unable to update the PDP context in one or more GGSNs, the new SGSN shall deactivate the corresponding PDP contexts as described in subclause "SGSN-initiated PDP Context Deactivation Procedure". This shall not cause the SGSN to reject the routeing area update.

The PDP Contexts shall be sent from old to new SGSN in a prioritized order, i.e. the most important PDP Context first in the SGSN Context Response message. (The prioritization method is implementation dependent, but should be based on the current activity.)

If the new SGSN is unable to support the same number of active PDP contexts as received from old SGSN, the new SGSN should use the prioritisation sent by old SGSN as input when deciding which PDP contexts to maintain active and which ones to delete. PDP contexts related to an emergency use shall have a high priority and therefore PDP contexts for emergency use should not be deactivated during the routeing area update. In any case, the new SGSN shall first update all contexts in one or more GGSNs and then deactivate the context(s) that it cannot maintain as described in subclause "SGSN-initiated PDP Context Deactivation Procedure". This shall not cause the SGSN to reject the routeing area update.

The CAMEL procedure calls shall be performed, see referenced procedures in TS 23.078:

C1) CAMEL_GPRS_PDP_Context_Disconnection, CAMEL_GPRS_Detach and CAMEL_PS_Notification.

They are called in the following order:

- The CAMEL_GPRS_PDP_Context_Disconnection procedure is called several times: once per PDP context. The procedure returns as result "Continue".
- Then the CAMEL_GPRS_Detach procedure is called once. It returns as result "Continue".
- Then the CAMEL_PS_Notification procedure is called once. It returns as result "Continue".

C2) CAMEL_GPRS_Routeing_Area_Update_Session and CAMEL_PS_Notification.

They are called in the following order:

- The CAMEL_GPRS_Routeing_Area_Update_Session procedure is called. The procedure returns as result "Continue".
- Then the CAMEL_PS_Notification procedure is called. The procedure returns as result "Continue".

C3) CAMEL_GPRS_Routeing_Area_Update_Context

This procedure is called several times: once per PDP context. It returns as result "Continue".

6.2.7 Session Management Functionality

A GPRS-attached MS can initiate the activation, modification, and deactivation functions at any time for a PDP context in the MS, the SGSN, and the GGSN. A GGSN may request the activation of a PDP context to a GPRS-attached subscriber. A GGSN may initiate the deactivation of a PDP context.

NOTE: If the MS is in PMM-IDLE state, it needs to perform a service request procedure to enter the PMM-CONNECTED state before initiating these procedures.

Upon receiving an Activate PDP Context Request message or an Activate Secondary PDP Context Request message, the SGSN shall initiate procedures to set up PDP contexts. The first procedure includes subscription checking, APN selection, and host configuration, while the latter procedure excludes these functions and reuses PDP context parameters including the PDP address but except the QoS parameters. Once activated, all PDP contexts that share the same PDP address and APN shall be managed equally. At least one PDP context shall be activated for a PDP address before a

Secondary PDP Context Activation procedure may be initiated. When the MS performs an RA update procedure to change from a release 99 to a release 97 or 98 system, only one active PDP context per PDP address and APN shall be preserved. This PDP context is selected taking the QoS profile and NSAPI value into account.

Upon receiving a Deactivate PDP Context Request message, the SGSN shall initiate procedures to deactivate the PDP context. When the last PDP context associated with a PDP address is deactivated, N-PDU transfer for this PDP address is disabled.

An MS does not have to receive the (De-) Activate PDP Context Accept message before issuing another (De-)Activate PDP Context Request. However, only one request can be outstanding for every TI.

By sending a RAB Release Request or Iu Release Request message to the SGSN, the RAN initiates the release of one or more RABs. The preservation function allows the active PDP contexts associated with the released RABs to be preserved without modification in the CN, and the RABs can then be re-established at a later stage.

Upon receiving an Activate PDP Context Request message with a globally dedicated emergency APN or a related Activate Secondary PDP Context Request message, the SGSN shall initiate procedures to set up PDP contexts and may give special treatment.

Upon receiving an Activate PDP Context Request message without the globally dedicated emergency APN from an MS that is emergency attached, the SGSN shall reject the request and respond with an appropriate cause.

PDP contexts related to an emergency use shall have a high priority therefore in case of congestion or when the SGSN is unable to support all requested PDP contexts, PDP contexts related to an emergency use should not be deactivated.

6.2.7.1 PDP Context Activation

6.2.7.1.1 PDP Context Activation Procedure

The PDP Context Activation procedure is illustrated in figure 6.13 and figure 6.14.

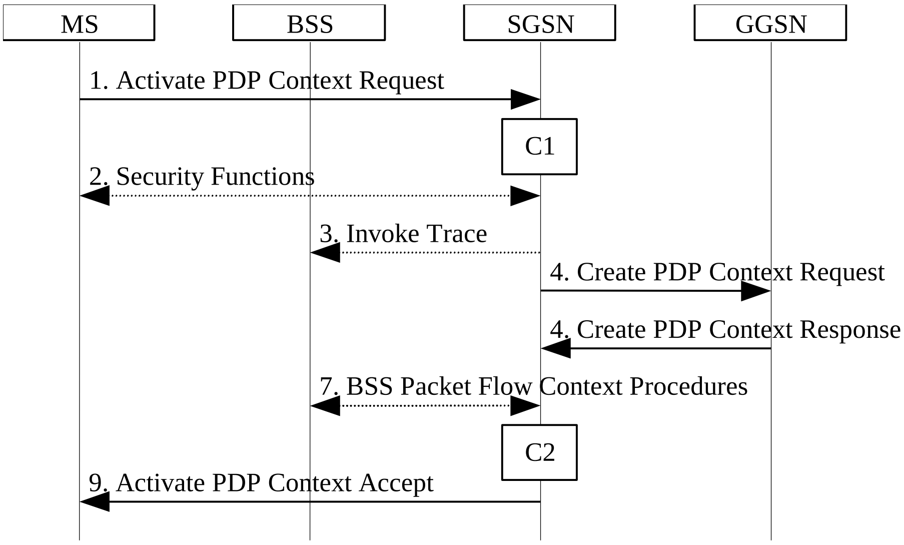
MS
BSS
SGSN
GGSN
1. Activate PDP Context Request
C1
2. Security Functions
3. Invoke Trace
4. Create PDP Context Request
4. Create PDP Context Response
7. BSS Packet Flow Context Procedures
C2
9. Activate PDP Context Accept

Figure 6.13: PDP Context Activation Procedure for A/Gb mode

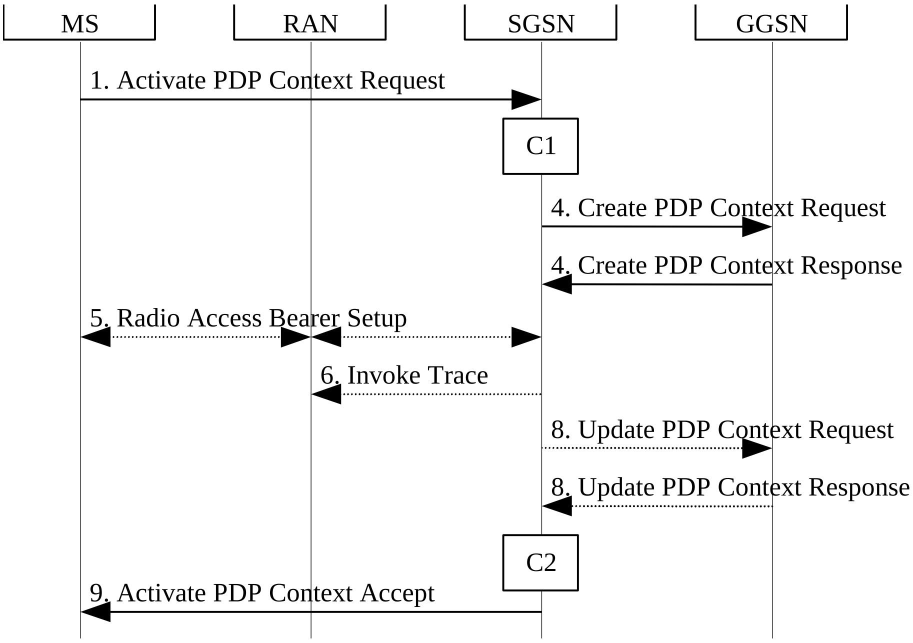
MS
RAN
SGSN
GGSN
1. Activate PDP Context Request
C1
4. Create PDP Context Request
4. Create PDP Context Response
5. Radio Access Bearer Setup
6. Invoke Trace
8. Update PDP Context Request
8. Update PDP Context Response
C2
9. Activate PDP Context Accept

Figure 6.14: PDP Context Activation Procedure for Iu mode

1) The MS sends an Activate PDP Context Request (NSAPI, TI, PDP Type, PDP Address, Access Point Name, QoS Requested, PDP Configuration Options) message to the SGSN. The MS shall use PDP Address to indicate whether it requires the use of a static PDP address or whether it requires the use of a dynamic PDP address. The MS shall leave PDP Address empty to request a dynamic PDP address. The MS shall use the globally dedicated emergency Access Point Name to indicate emergency access to the PS domain. Access Point Name is a logical name referring to the packet data network and/or to a service that the subscriber wishes to connect to. QoS Requested indicates the desired QoS profile. PDP Configuration Options may be used to transfer optional PDP parameters and/or request to the GGSN (see GSM 29.060 [26] and 24.229 [75]). PDP Configuration Options is sent transparently through the SGSN. The MS shall use the globally dedicated Access Point Name, if the PDP context is for emergency use.

2) In A/Gb mode, security functions may be executed. These procedures are defined in clause "Security Function".

3) In A/Gb mode and if BSS trace is activated, the SGSN shall send an Invoke Trace (Trace Reference, Trace Type, Trigger Id, OMC Identity) message to the BSS. Trace Reference, and Trace Type are copied from the trace information received from the HLR or OMC.

4) The SGSN validates the Activate PDP Context Request using PDP Type (optional), PDP Address (optional), and Access Point Name provided by the MS and the PDP context subscription records. The validation criteria, the APN selection criteria, and the mapping from APN to a GGSN are described in annex A.

   If no GGSN address can be derived or if the SGSN has determined that the Activate PDP Context Request is not valid according to the rules described in annex A, the SGSN rejects the PDP context activation request.

   If a GGSN address can be derived, the SGSN creates a TEID for the requested PDP context. If the MS requests a dynamic address, the SGSN lets a GGSN allocate the dynamic address. The SGSN may restrict the requested QoS attributes given its capabilities and the current load, and it shall restrict the requested QoS attributes according to the subscribed QoS profile.

   The SGSN sends a Create PDP Context Request (PDP Type, PDP Address, Access Point Name, QoS Negotiated, TEID, NSAPI, MSISDN, Selection Mode, Charging Characteristics, Trace Reference, Trace Type, Trigger Id, OMC Identity, PDP Configuration Options) message to the affected GGSN. Access Point Name shall be the APN Network Identifier of the APN selected according to the procedure described in Annex A. PDP Address shall be empty if a dynamic address is requested. The GGSN may use Access Point Name to find a packet data network and optionally to activate a service for this APN. Selection Mode indicates whether a subscribed APN was selected, or whether a non-subscribed APN sent by an MS or a non-subscribed APN chosen by the SGSN was selected. Selection Mode is set according to Annex A. The GGSN may use Selection Mode when deciding whether to accept or reject the PDP context activation. For example, if an APN requires subscription, the GGSN is configured to accept only the PDP context activation that requests a subscribed APN as indicated by the SGSN with Selection Mode. The dedicated emergency APN does not require any subscription. Charging Characteristics indicates which kind of charging the PDP context is liable for. The charging characteristics on the GPRS subscription and individually subscribed APNs as well as the way the SGSN handles Charging Characteristics and chooses to send them or not to the GGSN is defined in TS 32.215. The SGSN shall include Trace Reference, Trace Type, Trigger Id, and OMC Identity if GGSN trace is activated. The SGSN shall copy Trace Reference, Trace Type, and OMC Identity from the trace information received from the HLR or OMC.

The GGSN creates a new entry in its PDP context table and generates a Charging Id. The new entry allows the GGSN to route PDP PDUs between the SGSN and the packet data network, and to start charging. The way the GGSN handles Charging Characteristics that it may have received from the SGSN is defined in TS 32.215. The GGSN may restrict QoS Negotiated given its capabilities and the current load. The GGSN then returns a Create PDP Context Response (TEID, PDP Address, PDP Configuration Options, QoS Negotiated, Charging Id, Cause) message to the SGSN. PDP Address is included if the GGSN allocated a PDP address. If the GGSN has been configured by the operator to use External PDN Address Allocation for the requested APN, PDP Address shall be set to 0.0.0.0, indicating that the PDP address shall be negotiated by the MS with the external PDN after completion of the PDP Context Activation procedure. The GGSN shall relay, modify and monitor these negotiations as long as the PDP context is in ACTIVE state, and use the GGSN-Initiated PDP Context Modification procedure to transfer the currently used PDP address to the SGSN and the MS. PDP Configuration Options contain optional PDP parameters that the GGSN may transfer to the MS. These optional PDP parameters may be requested by the MS in the Activate PDP Context Request message, or may be sent unsolicited by the GGSN. PDP Configuration Options is sent transparently through the SGSN. The Create PDP Context messages are sent over the backbone network.

If QoS Negotiated received from the SGSN is incompatible with the PDP context being activated, the GGSN rejects the Create PDP Context Request message. The GGSN operator configures the compatible QoS profiles.

5) In Iu mode, RAB setup is done by the RAB Assignment procedure, see subclause "RAB Assignment Procedure".

6) In Iu mode and if BSS trace is activated, the SGSN shall send an Invoke Trace (Trace Reference, Trace Type, Trigger Id, OMC Identity) message to the RAN. Trace Reference, and Trace Type are copied from the trace information received from the HLR or OMC.

7) In A/Gb mode, BSS packet flow context procedures may be executed. These procedures are defined in clause "BSS Context".

8) In Iu mode and in case the QoS attributes have been downgraded in step 5, the SGSN may inform the GGSN about the downgraded QoS attributes by sending an Update PDP Context Request to the affected GGSN. The GGSN confirms the new QoS attributes by sending an Update PDP Context Response to the SGSN.

9) The SGSN inserts the NSAPI along with the GGSN address in its PDP context. If the MS has requested a dynamic address, the PDP address received from the GGSN is inserted in the PDP context. The SGSN selects Radio Priority and Packet Flow Id based on QoS Negotiated, and returns an Activate PDP Context Accept (PDP Type, PDP Address, TI, QoS Negotiated, Radio Priority, Packet Flow Id, PDP Configuration Options) message to the MS. PDP Configuration Options may be used to transfer optional PDP parameters to the UE (see GSM 29.060 [26] and 24.229 [75]). PDP Configuration Options is sent transparently through the SGSN.The SGSN is now able to route PDP PDUs between the GGSN and the MS, and to start charging.

For each PDP Address a different quality of service (QoS) profile may be requested. For example, some PDP addresses may be associated with E-mail that can tolerate lengthy response times. Other applications cannot tolerate delay and demand a very high level of throughput, interactive applications being one example. These different requirements are reflected in the QoS profile. The QoS profile is defined in clause "Quality of Service Profile". If a QoS requirement is beyond the capabilities of a PLMN, the PLMN negotiates the QoS profile as close as possible to the requested QoS profile. The MS either accepts the negotiated QoS profile, or deactivates the PDP context.

After an SGSN has successfully updated the GGSN, the PDP contexts associated with an MS is distributed as shown in clause "Information Storage".

If the PDP Context Activation Procedure fails or if the SGSN returns an Activate PDP Context Reject (Cause, PDP Configuration Options) message, the MS may attempt another activation to the same APN up to a maximum number of attempts.

The CAMEL procedure calls shall be performed, see referenced procedures in TS 23.078:

C1) CAMEL_GPRS_PDP_Context_Establishment.

In Figure 6.13 and Figure 6.14, procedures return as result "Continue".

C2) CAMEL_GPRS_PDP_Context_Establishment_Acknowledgement.

In Figure 6.13 and Figure 6.14, procedures return as result "Continue".

6.2.7.1.2 Secondary PDP Context Activation Procedure

The Secondary PDP Context Activation procedure may be used to activate a PDP context while reusing the PDP address and other PDP context information from an already active PDP context, but with a different QoS profile. Procedures for APN selection and PDP address negotiation are not executed. A unique TI and a unique NSAPI shall identify each PDP context sharing the same PDP address and APN.

The Secondary PDP Context Activation procedure may be executed without providing a Traffic Flow Template (TFT) to the newly activated PDP context if all other active PDP contexts for this PDP address and APN already have an associated TFT. Otherwise a TFT shall be provided. The TFT contains attributes that specify an IP header filter that is used to direct data packets received from the interconnected packet data network to the newly activated PDP context.

The Secondary PDP Context Activation procedure may only be initiated after a PDP context is already activated for the same PDP address and APN. The procedure is illustrated in Figure 6.15 and Figure 6.16.

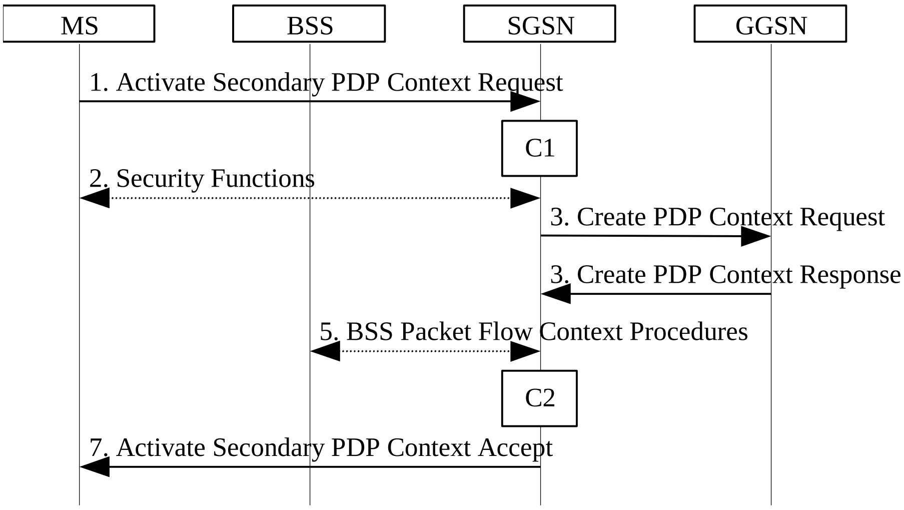
MS
BSS
SGSN
GGSN
1. Activate Secondary PDP Context Request
C1
2. Security Functions
3. Create PDP Context Request
3. Create PDP Context Response
5. BSS Packet Flow Context Procedures
C2
7. Activate Secondary PDP Context Accept

Figure 6.15: Secondary PDP Context Activation Procedure for A/Gb mode

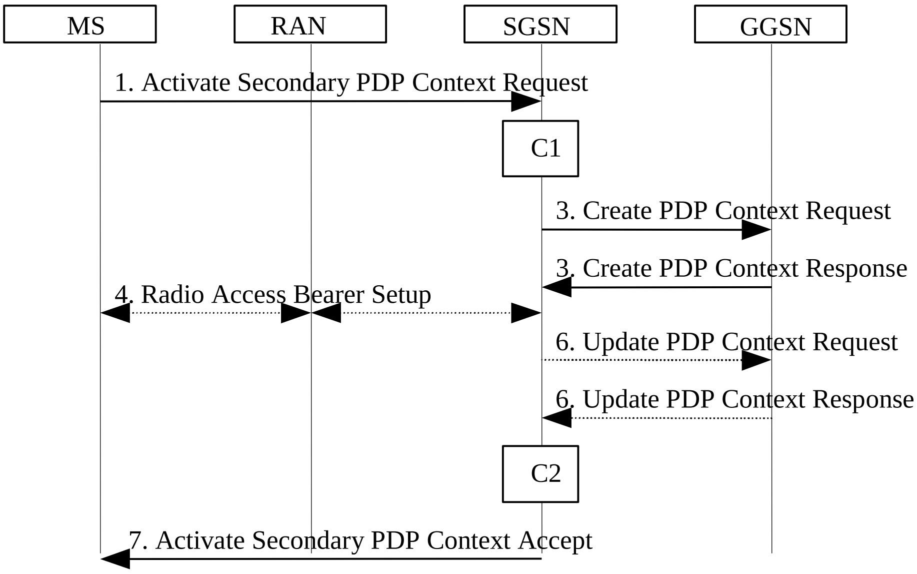
MS
RAN
SGSN
GGSN
1. Activate Secondary PDP Context Request
C1
3. Create PDP Context Request
3. Create PDP Context Response
4. Radio Access Bearer Setup
6. Update PDP Context Request
6. Update PDP Context Response
C2
7. Activate Secondary PDP Context Accept

Figure 6.16: Secondary PDP Context Activation Procedure for Iu mode

1) The MS sends an Activate Secondary PDP Context Request (Linked TI, NSAPI, TI, QoS Requested, TFT, PDP Configuration Options) message to the SGSN. Linked TI indicates the TI value assigned to any one of the already activated PDP contexts for this PDP address and APN. QoS Requested indicates the desired QoS profile. TFT is sent transparently through the SGSN to the GGSN to enable packet classification for downlink data transfer. TI and NSAPI contain values not used by any other activated PDP context. PDP Configuration Options may be used to transfer optional PDP parameters and/or requests to the GGSN (see GSM 29.060 [26] and 24.229 [75]). PDP Configuration Options is sent transparently through the SGSN.

2) In A/Gb mode, security functions may be executed. These procedures are defined in clause "Security Function".

3) The SGSN validates the Activate Secondary PDP Context Request using the TI indicated by Linked TI. The same GGSN address is used by the SGSN as for the already-activated PDP context(s) for that TI and PDP address.

   The SGSN may restrict the requested QoS attributes given its capabilities and the current load, and it shall restrict the requested QoS attributes according to the subscribed QoS profile, which represents the maximum QoS per PDP context to the associated APN. The GGSN may restrict and negotiate the requested QoS as specified in clause "PDP Context Activation Procedure". The SGSN sends a Create PDP Context Request (QoS Negotiated, TEID, NSAPI, Primary NSAPI, TFT, PDP Configuration Options) message to the affected GGSN. Primary NSAPI indicates the NSAPI value assigned to any one of the already activated PDP contexts for this PDP address and APN. TFT is included only if received in the Activate Secondary PDP Context Request message. PDP Configuration Options is sent transparently through the SGSN if received in the Activate secondary PDP Context Request message.

   The GGSN uses the same packet data network as used by the already-activated PDP context(s) for that PDP address, generates a new entry in its PDP context table, and stores the TFT. The new entry allows the GGSN to route PDP PDUs via different GTP tunnels between the SGSN and the packet data network. The GGSN returns a Create PDP Context Response (TEID, QoS Negotiated, Cause, PDP Configuration Options) message to the SGSN. PDP Configuration Options may be used to transfer optional PDP parameters to the UE (see GSM 29.060 [26] and 24.229 [75]).

4) In Iu mode, RAB setup is done by the RAB Assignment procedure.

5) In A/Gb mode, BSS packet flow context procedures may be executed. These procedures are defined in clause "BSS Context".

6) In Iu mode and in case the QoS attributes have been downgraded in step 4, the SGSN may inform the GGSN about the downgraded QoS attributes by sending an Update PDP Context Request to the affected GGSN. The GGSN confirms the new QoS attributes by sending an Update PDP Context Response to the SGSN.

7) The SGSN selects Radio Priority and Packet Flow Id based on QoS Negotiated, and returns an Activate Secondary PDP Context Accept (TI, QoS Negotiated, Radio Priority, Packet Flow Id, PDP Configuration

Options) message to the MS. PDP Configuration Options is sent transparently through the SGSN if received in the Create PDP Context Response message. The SGSN is now able to route PDP PDUs between the GGSN and the MS via different GTP tunnels and possibly different LLC links.

For each additionally activated PDP context a QoS profile and TFT may be requested.

If the secondary PDP context activation procedure fails or if the SGSN returns an Activate Secondary PDP Context Reject (Cause, PDP Configuration Options) message, the MS may attempt another activation with a different TFT, depending on the cause.

The CAMEL procedure calls shall be performed, see referenced procedures in TS 23.078:

C1) CAMEL_GPRS_PDP_Context_Establishment.

In Figure 6.15 and in Figure 6.16, procedures return as result "Continue".

C2) CAMEL_GPRS_PDP_Context_Establishment_Acknowledgement.

In Figure 6.15 and in Figure 6.16, procedures return as result "Continue".

6.2.7.2 PDP Context Modification

Normal procedures according to 23.060 [2] are applicable also for PDP contexts towards emergency APN.

6.2.7.3 PDP Context Deactivation

Normal procedures according to 23.060 [2] are applicable also for PDP contexts towards emergency APN.

6.2.7.4 Preservation Functions

Normal procedures according to 23.060 [2] are applicable also for PDP contexts towards emergency APN.

6.2.8 Information Storage

6.2.8.1 SGSN

SGSN maintains MM context and PDP context information for MSs in the STANDBY, READY, PMM-IDLE, and PMM-CONNECTED states. Table 1 shows the context fields for one MS.

During the Intersystem Change, when new Authentication and Key Agreement is not performed, the KSI in the new 3G-SGSN shall be assigned the value of the CKSN, which has been sent by the MS. Similarly, in the new 2G-SGSN, when AKA does not take place, the CKSN shall be assigned the value of the KSI, which has been sent by the MS.

Table 1: SGSN MM and PDP Contexts

Field	Description	A/Gb mode	Iu mode
IMSI	IMSI is the main reference key.	X	X
MM State	Mobility management state, IDLE, STANDBY, READY, PMM-DETACHED, PMM-IDLE, or PMM-CONNECTED.	X	X
P-TMSI	Packet Temporary Mobile Subscriber Identity.	X	X
P-TMSI Signature	A signature used for identification checking purposes.	X	X
IMEI	International Mobile Equipment Identity	X	X
MSISDN	The basic MSISDN of the MS.	X	X
Routeing Area	Current routeing area.	X	X
Cell Identity	Current cell in READY state, last known cell in STANDBY or IDLE state.	X	
Cell Identity Age	Time elapsed since the last LLC PDU was received from the MS at the SGSN.	X	
Service Area Code	Last known SAC when initial UE message was received or Location Reporting procedure was executed.		X
Service Area Code Age	Time elapsed since the last SAC was received at the 3G-SGSN.		X
VLR Number	The VLR number of the MSC/VLR currently serving this MS.	X	X
New SGSN Address	The IP address of the new SGSN where buffered and not sent N-PDUs should be forwarded to.	X	X
Authentication Vectors	Authentication and ciphering parameters (authentication triplets or quintets)..	X	X
Kc	Currently used A/Gb mode ciphering key.	X	2)
CKSN	Ciphering key sequence number of Kc.	X	2)
Ciphering algorithm	Selected ciphering algorithm.	X	X
CK	Currently used Iu mode ciphering key.	1)	X
IK	Currently used Iu mode integrity key.	1)	X
KSI	Key Set Identifier.	1)	X
MS Radio Access Capability	MS radio access capabilities.	X	
MS Network Capability	MS network capabilities.	X	X
DRX Parameters	Discontinuous reception parameters.	X	X
MNRG	Indicates whether activity from the MS shall be reported to the HLR.	X	X
NGAF	Indicates whether activity from the MS shall be reported to the MSC/VLR.	X	X
PPF	Indicates whether paging for PS and CS services can be initiated.	X	X
Subscribed Charging Characteristics	The charging characteristics for the MS, e.g. normal, prepaid, flat-rate, and/or hot billing subscription.	X	X
Trace Reference	Identifies a record or a collection of records for a particular trace.	X	X
Trace Type	Indicates the type of trace.	X	X
Trigger Id	Identifies the entity that initiated the trace.	X	X
OMC Identity	Identifies the OMC that shall receive the trace record(s).	X	X
SMS Parameters	SMS-related parameters, e.g. operator-determined barring.	X	X
Recovery	Indicates if HLR or VLR is performing database recovery.	X	X
Radio Priority SMS	The RLC/MAC radio priority level for uplink SMS transmission.	X	
GPRS-CSI	Optional GPRS CAMEL subscription information, see TS 23.016	X	X
MG-CSI	Optional Mobility Management for GPRS CAMEL subscription information, see TS 23.016.	X	X
ODB for PS parameters	Indicates that the status of the operator determined barring for packet oriented services.	X	X
Emergency Indication	Indicates that MS has been Attached for Emergency use.	X	X
Each MM context contains zero or more of the following PDP contexts:			
PDP Context Identifier	Index of the PDP context.	X	X
PDP State	Packet data protocol state, INACTIVE or ACTIVE.	X	X
PDP Type	PDP type, e.g. PPP or IP.	X	X
PDP Address	PDP address, e.g. an IP address.	X	X
APN Subscribed	The APN received from the HLR.	X	X
APN in Use	The APN currently used. This APN shall be composed of the APN Network Identifier and the APN Operator Identifier.	X	X
NSAPI	Network layer Service Access Point Identifier.	X	X
TI	Transaction Identifier.	X	X
TEID for Gn/Gp	Tunnel Endpoint Identifier for the Gn and Gp interfaces.	X	X
TEID for Iu	Tunnel Endpoint Identifier for the Iu interface.		X
GGSN Address in Use	The IP address of the GGSN currently used.	X	X
VPLMN Address Allowed	Specifies whether the MS is allowed to use the APN in the domain of the HPLMN only, or additionally the APN in the domain of the	X	X

Field	Description	A/Gb mode	Iu mode
	VPLMN.		
QoS Profile Subscribed	The quality of service profile subscribed.	X	X
QoS Profile Requested	The quality of service profile requested.	X	X
QoS Profile Negotiated	The quality of service profile negotiated.	X	X
Radio Priority	The RLC/MAC radio priority level for uplink user data transmission.	X	
Packet Flow Id	Packet flow identifier.	X	
Aggregate BSS QoS Profile Negotiated	The aggregate BSS quality of service profile negotiated for the packet flow that this PDP context belongs to.	X	
Send N-PDU Number	SNDCP sequence number of the next downlink N-PDU to be sent to the MS.	X	
Receive N-PDU Number	SNDCP sequence number of the next uplink N-PDU expected from the MS.	X	
GTP-SND	GTP-U sequence number of the next downlink N-PDU to be sent to the MS.	X	X
GTP-SNU	GTP-U sequence number of the next uplink N-PDU to be sent to the GGSN.	X	X
PDCP-SND	Sequence number of the next downlink in-sequence PDCP-PDU to be sent to the MS.		X
PDCP-SNU	Sequence number of the next uplink in-sequence PDCP-PDU expected from the MS.		X
Charging Id	Charging identifier, identifies charging records generated by SGSN and GGSN.	X	X
PDP Context Charging Characteristics	The charging characteristics of this PDP context, e.g. normal, prepaid, flat-rate, and/or hot billing.	X	X
RNC Address in Use	The IP address of the RNC/BSC currently used.		X

The information marked with a "1)" in table 1 may be maintained if authentication is performed by the UMTS authentication procedure.

The information marked with a "2)" in table 1 may be maintained if authentication is performed by the GSM authentication procedure.

6.2.8.2 GGSN

GGSN maintains activated PDP contexts. Table 2 shows the PDP context fields for one PDP Address.

Table 2: GGSN PDP Context

Field	Description
IMSI	International Mobile Subscriber Identity.
NSAPI	Network layer Service Access Point Identifier.
MSISDN	The basic MSISDN of the MS.
PDP Type	PDP type; e.g. PPP or IP.
PDP Address	PDP address; e.g. an IP address.
Dynamic Address	Indicates whether PDP Address is static or dynamic.
APN in Use	The APN Network Identifier currently used.
TEID	Tunnel Endpoint Identifier.
TFT	Traffic flow template.
QoS Profile Negotiated	The quality of service profile negotiated.
SGSN Address	The IP address of the SGSN currently serving this MS.
MNRG	Indicates whether the MS is marked as not reachable for PS at the HLR.
Recovery	Indicates if the SGSN is performing database recovery.
GTP-SND	GTP-U sequence number of the next downlink N-PDU to be sent to the SGSN.
GTP-SNU	GTP-U sequence number of the next uplink N-PDU to be received from the SGSN.
Charging Id	Charging identifier, identifies charging records generated by SGSN and GGSN.
Charging Characteristics	The charging characteristics for this PDP context, e.g. normal, prepaid, flat-rate, and/or hot billing.
Trace Reference	Identifies a record or a collection of records for a particular trace.
Trace Type	Indicates the type of trace.
Trigger Id	Identifies the entity that initiated the trace.
OMC Identity	Identifies the OMC that shall receive the trace record(s).

If a PDP context is enabled for network-requested PDP context activation, then IMSI, PDP Type, PDP Address, SGSN Address and MNRG contain valid information also when the PDP context is inactive and when the MS is GPRS-detached.

6.2.8.3 MS

Each MS supporting GPRS maintains MM and PDP context information in IDLE, STANDBY, READY, PMM-DETACHED, PMM-IDLE, and PMM-CONNECTED states. The information may be contained in the MS and the TE. Table 3 shows the MS context fields.

Table 3: MS MM and PDP Contexts

Field	SIM	Description	A/Gb mode	Iu mode
IMSI	G, U	International Mobile Subscriber Identity.	X	X
MM State		Mobility management state, IDLE, STANDBY, READY, PMM-DETACHED, PMM-IDLE, or PMM-CONNECTED.	X	X
P-TMSI	G, U	Packet Temporary Mobile Subscriber Identity.	X	X
P-TMSI Signature	G, U	A signature used for identification checking purposes.	X	X
Routeing Area	G, U	Current routeing area.	X	X
Cell Identity		Current cell.	X	
Kc	G	Current A/Gb mode ciphering key.	X	2)
KSI / CKSN	G, U	Key Set Identifier for IK Next, CK Next / key sequence number of Kc.	X	X
Ciphering algorithm		Selected ciphering algorithm.	X	X
CK		Currently used Iu mode ciphering key.	1)	X
CK Next	U	Iu mode ciphering key to be used after the next security mode command.	1)	X
IK		Currently used Iu mode integrity key.	1)	X
IK Next	U	Integrity key to be used after the next security mode command.	1)	X
MS Radio Access Capability		MS radio access capabilities.	X	X
UE Capability		UE radio capabilities.		X
MS Network Capability		MS network capabilities.	X	X
DRX Parameters		Discontinuous reception parameters.	X	X
Radio Priority SMS		The RLC/MAC radio priority level for uplink SMS transmission.	X	
Emergency Indication		Indicates that MS has been Attached for Emergency use.	X	X
Each MM context contains zero or more of the following PDP contexts:				
PDP Type		PDP type, e.g. PPP or IP.	X	X
PDP Address		PDP address; e.g. an IP address.	X	X
PDP State		Packet data protocol state, INACTIVE or ACTIVE.	X	X
Dynamic Address Allowed		Specifies whether the MS is allowed to use a dynamic address.	X	X
APN Requested		The APN requested.	X	X
NSAPI		Network layer Service Access Point Identifier.	X	X
TI		Transaction Identifier.	X	X
QoS Profile Requested		The quality of service profile requested.	X	X
QoS Profile Negotiated		The quality of service profile negotiated.	X	X
TFT		Traffic flow template.	X	X
Radio Priority		The RLC/MAC radio priority level for uplink user data transmission.	X	
Packet Flow Id		Packet flow identifier.	X	
Send N-PDU Number		SNDCP sequence number of the next uplink N-PDU to be sent to the SGSN.	X	X
Receive N-PDU Number		SNDCP sequence number of the next downlink N-PDU expected from the SGSN.	X	X
PDCP-SND		Sequence number of the next downlink in-sequence PDCP-PDU expected from the RNC.		X
PDCP-SNU		Sequence number of the next uplink in-sequence PDCP-PDU to be sent to the RNC.		X

6.3 General Packet Radio Service (GPRS) for UICC-less case

6.3.1 GPRS Attach Function and PDP Context Activation Procedure

The following procedure is used if the UICC is not valid or does not exist and the IMEI is used instead of the IMSI to identify the calling subscriber.

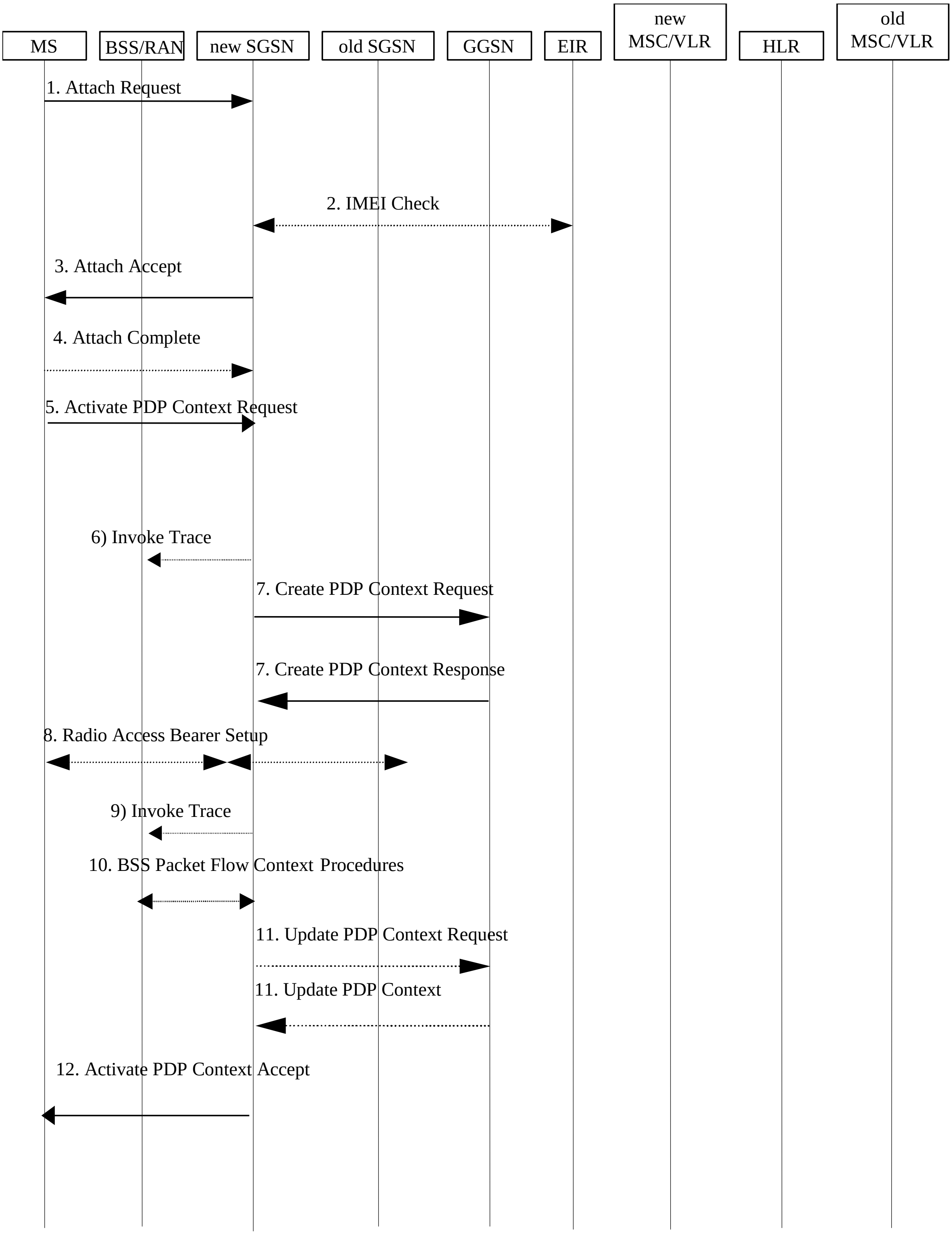
MS
BSS/RAN
new SGSN
old SGSN
GGSN
EIR
new MSC/VLR
HLR
old MSC/VLR
1. Attach Request
2. IMEI Check
3. Attach Accept
4. Attach Complete
5. Activate PDP Context Request
6) Invoke Trace
7. Create PDP Context Request
7. Create PDP Context Response
8. Radio Access Bearer Setup
9) Invoke Trace
10. BSS Packet Flow Context Procedures
11. Update PDP Context Request
11. Update PDP Context
12. Activate PDP Context Accept

Figure 6.17: GPRS Attach Function and PDP Context Activation Procedure in the UICC-less case

1) In A/Gb mode, the MS initiates the attach procedure by the transmission of an Attach Request (IMEI, Classmark, Attach Type , DRX Parameters, Emergency Indication) message to the SGSN. IMEI shall be included, as the MS does not have a valid IMSI or P-TMSI available. Classmark contains the MS's GPRS multislot capabilities and supported GPRS ciphering algorithms in addition to the existing classmark parameters defined in GSM 04.08. Attach Type indicates which type of attach is to be performed, i.e. GPRS attach only. DRX Parameters indicates whether the MS uses discontinuous reception or not. If the MS uses discontinuous reception, then DRX Parameters also indicate when the MS is in a non-sleep mode able to receive paging requests and channel assignments.

   For Iu mode, the MS initiates the attach procedure by the transmission of an Attach Request (IMEI, Core Network Classmark, Attach Type, Follow On Request, DRX Parameters) message to the SGSN. IMEI shall be included, as the MS does not have a valid P-TMSI available. Core Network Classmark is described in clause "MS Network Capability". The MS shall set "Follow On Request Pending" as it has pending uplink traffic (emergency PDP context activation towards emergency APN). The SGSN shall use the follow on request pending indication to keep the Iu connection after the completion of the GPRS Attach procedure. Attach Type indicates which type of attach is to be performed, i.e. GPRS attach only. DRX Parameters indicates whether or not the MS uses discontinuous reception and the DRX cycle length.

   When the Attach is requested for emergency use, the MS shall include an Emergency Indication in the Attach Request.

2) The equipment checking functions are defined in the clause "Identity Check Procedures". Equipment checking is optional.

3) The SGSN selects Radio Priority SMS, and sends an Attach Accept (P-TMSI, P-TMSI Signature, Radio Priority SMS) message to the MS.

4) The MS acknowledges the received P-TMSI by returning an Attach Complete message to the SGSN.
   At any time after receiving Attach Complete, SGSN may initiate LCS procedure (i.e. PS-NI-LR). A simulated IMSI or IMEI is used to identify the target UE.

5) The MS sends an Activate PDP Context Request (NSAPI, TI, PDP Type, PDP Address, Access Point Name, QoS Requested, PDP Configuration Options) message to the SGSN. The MS shall use PDP Address to indicate whether it requires the use of a static PDP address or whether it requires the use of a dynamic PDP address. The MS shall leave PDP Address empty to request a dynamic PDP address. The MS shall use the globally dedicated emergency Access Point Name to indicate emergency access to the PS domain. Emergency PDP context activation towards any other APN other than emergency APN is not allowed after UICC-less Attach. This can be ensured by SGSN having a policy to reject PDP context activations towards any other APN than emergency APN after UE has made emergency attach. Access Point Name is a logical name referring to the packet data network and/or to a service that the subscriber wishes to connect to. QoS Requested indicates the desired QoS profile. PDP Configuration Options may be used to transfer optional PDP parameters and/or request to the GGSN (see GSM 29.060 [26] and 24.229 [75]). PDP Configuration Options is sent transparently through the SGSN. The MS shall use the globally dedicated emergency Access Point Name.

6) In A/Gb mode and if BSS trace is activated, the SGSN shall send an Invoke Trace (Trace Reference, Trace Type, Trigger Id, OMC Identity) message to the BSS. Trace Reference, and Trace Type are copied from the trace information received from the HLR or OMC.

7) The SGSN validates the Activate PDP Context Request using PDP Type (optional), PDP Address (optional), and Access Point Name provided by the MS and the PDP context subscription records. The validation criteria, the APN selection criteria, and the mapping from APN to a GGSN are described in annex A. The SGSN shall include "Emergency APN" in the APN selection criteria, in order to restrict access to APNs other than the emergency APN.

NOTE: When a CR to 23.060 is issued, annex A must reflect emergency APN handling as well.

   If no GGSN address can be derived or if the SGSN has determined that the Activate PDP Context Request is not valid according to the rules described in annex A, the SGSN rejects the PDP context activation request.

   If a GGSN address can be derived, the SGSN creates a TEID for the requested PDP context. If the MS requests a dynamic address, the SGSN lets a GGSN allocate the dynamic address. The SGSN may restrict the requested QoS attributes given its capabilities and the current load.

The SGSN sends a Create PDP Context Request (PDP Type, PDP Address, Access Point Name, QoS Negotiated, TEID, NSAPI, MSISDN, Selection Mode, Charging Characteristics, Trace Reference, Trace Type, Trigger Id, OMC Identity, PDP Configuration Options) message to the affected GGSN. Access Point Name shall be the APN Network Identifier of the APN selected according to the procedure described in Annex A. PDP Address shall be empty if a dynamic address is requested. The GGSN may use Access Point Name to find a packet data network and optionally to activate a service for this APN. Selection Mode indicates whether a subscribed APN was selected, or whether a non-subscribed APN sent by an MS or a non-subscribed APN chosen by the SGSN was selected. Selection Mode is set according to non-subscribed APN. The GGSN may use Selection Mode when deciding whether to accept or reject the PDP context activation. For example, if an APN requires subscription, the GGSN is configured to accept only the PDP context activation that requests a subscribed APN as indicated by the SGSN with Selection Mode. The dedicated emergency APN does not require any subscription. Charging Characteristics indicates which kind of charging the PDP context is liable for. The charging characteristics on the GPRS subscription and individually subscribed APNs as well as the way the SGSN handles Charging Characteristics and chooses to send them or not to the GGSN is defined in TS 32.215. The SGSN shall include Trace Reference, Trace Type, Trigger Id, and OMC Identity if GGSN trace is activated. The SGSN shall copy Trace Reference, Trace Type, and OMC Identity from the trace information received from the HLR or OMC.

The GGSN creates a new entry in its PDP context table and generates a Charging Id. The new entry allows the GGSN to route PDP PDUs between the SGSN and the packet data network, and to start charging. The way the GGSN handles Charging Characteristics that it may have received from the SGSN is defined in TS 32.215. The GGSN may restrict QoS Negotiated given its capabilities and the current load. The GGSN then returns a Create PDP Context Response (TEID, PDP Address, PDP Configuration Options, QoS Negotiated, Charging Id, Prohibit Payload Compression, Cause) message to the SGSN. The Prohibit Payload Compression indicates that the SGSN should negotiate no data compression for this PDP context. PDP Address is included if the GGSN allocated a PDP address. If the GGSN has been configured by the operator to use External PDN Address Allocation for the requested APN, PDP Address shall be set to 0.0.0.0, indicating that the PDP address shall be negotiated by the MS with the external PDN after completion of the PDP Context Activation procedure. The GGSN shall relay, modify and monitor these negotiations as long as the PDP context is in ACTIVE state, and use the GGSN-Initiated PDP Context Modification procedure to transfer the currently used PDP address to the SGSN and the MS. PDP Configuration Options contain optional PDP parameters that the GGSN may transfer to the MS. These optional PDP parameters may be requested by the MS in the Activate PDP Context Request message, or may be sent unsolicited by the GGSN. PDP Configuration Options is sent transparently through the SGSN. The Create PDP Context messages are sent over the backbone network.

If QoS Negotiated received from the SGSN is incompatible with the PDP context being activated, the GGSN rejects the Create PDP Context Request message. The GGSN operator configures the compatible QoS profiles.

8) In Iu mode, RAB setup is done by the RAB Assignment procedure, see subclause "RAB Assignment Procedure".

9) In Iu mode and if BSS trace is activated, the SGSN shall send an Invoke Trace (Trace Reference, Trace Type, Trigger Id, OMC Identity) message to the RAN. Trace Reference, and Trace Type are copied from the trace information received from the HLR or OMC.

10) In A/Gb mode, BSS packet flow context procedures may be executed. These procedures are defined in clause "BSS Context".

11) In case the QoS attributes have been downgraded in step 10 for A/Gb mode or in step 8 for Iu mode, the SGSN may inform the GGSN about the downgraded QoS attributes by sending an Update PDP Context Request to the affected GGSN. The GGSN confirms the new QoS attributes by sending an Update PDP Context Response to the SGSN.

12) The SGSN inserts the NSAPI along with the GGSN address in its PDP context. If the MS has requested a dynamic address, the PDP address received from the GGSN is inserted in the PDP context. The SGSN selects Radio Priority and Packet Flow Id based on QoS Negotiated, and returns an Activate PDP Context Accept (PDP Type, PDP Address, TI, QoS Negotiated, Radio Priority, Packet Flow Id, PDP Configuration Options) message to the MS. PDP Configuration Options may be used to transfer optional PDP parameters to the UE (see TS 29.060 [26] and TS 24.229 [75]). PDP Configuration Options is sent transparently through the SGSN. The SGSN is now able to route PDP PDUs between the GGSN and the MS, and to start charging.

6.3.2 GPRS Detach Function

In UICC less case, the MS shall initiate a GPRS detach after the emergency PDP contexts have been deactivated (i.e. once the emergency use is finished). In case that SGSN initiates the GPRS detach, an appropriate cause shall be sent to the MS.

6.3.3 Location Management Function

Location management procedures presented in chapters 6.2.3, 6.2.4, 6.2.5 and 6.2.6 are applicable also for the UICC-less case, with the following exceptions:

- Simulated IMSI or IMEI is used to identify the UE;
- Security functions shall not be performed;
- HLR dialog shall not be performed, if IMEI is used for identification;
- Camel procedures shall not be performed;
- Combined RA/LA update procedure shall not be performed (only periodic updating and RA updating shall be used for Update Type);
- MS shall keep the Iu connection up after the RAU (by setting Follow on Request Pending) as it has an emergency session ongoing that requires a signalling connection.

Annex A: Retrieval of Location Information for Emergency Services over Fixed Broadband Access

A.1 High Level Flows for the retrieval of location information for emergency services over fixed broadband access

When performing an emergency service, two possibilities for retrieving location information are considered. These are the "UE retrieves the location information" and "the IMS core retrieves the location information". The related high level procedures are described below. In both cases the access network needs to maintain and determine the location of the UE.

A.1.1 The UE acquires the location information

The terminal may determine its own location or it may retrieve the location information from the IP-CAN.

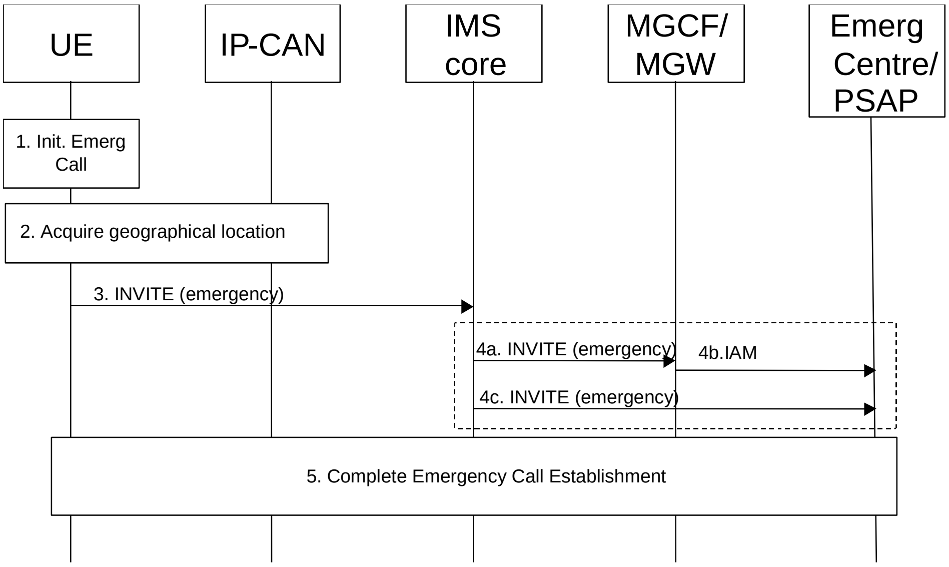

Figure A.1: Terminal requests location information from the IP-CAN

1. The user initiates an emergency call.

2. The UE determines its own location if possible. If the UE is not able to determine its own location, the UE requests the location from the IP-CAN. The IP-CAN returns a representation of the location information to the UE.

3. The user equipment sends an INVITE with an emergency indication and location information to the IMS core.

4. The IMS core selects an emergency centre or PSAP and sends the request including the location information to the emergency centre or PSAP.
   4a. The INVITE is sent to an MGCF/MGW, 4b. The IAM is continued towards the emergency centre or PSAP
   Or 4c. The INVITE is sent directly to the emergency centre or PSAP.

5. The emergency call establishment is completed.

A.1.2 The IMS core request the location information

The IMS-core may retrieve the location information either from the IP-CAN directly, or from a location retrieval function (LRF), which may be e.g. a AAA server in the core network.

NOTE: When the Retrieve Location request is sent directly to the IP-CAN, it is assumed that the location retrieval function is included within the IP-CAN.

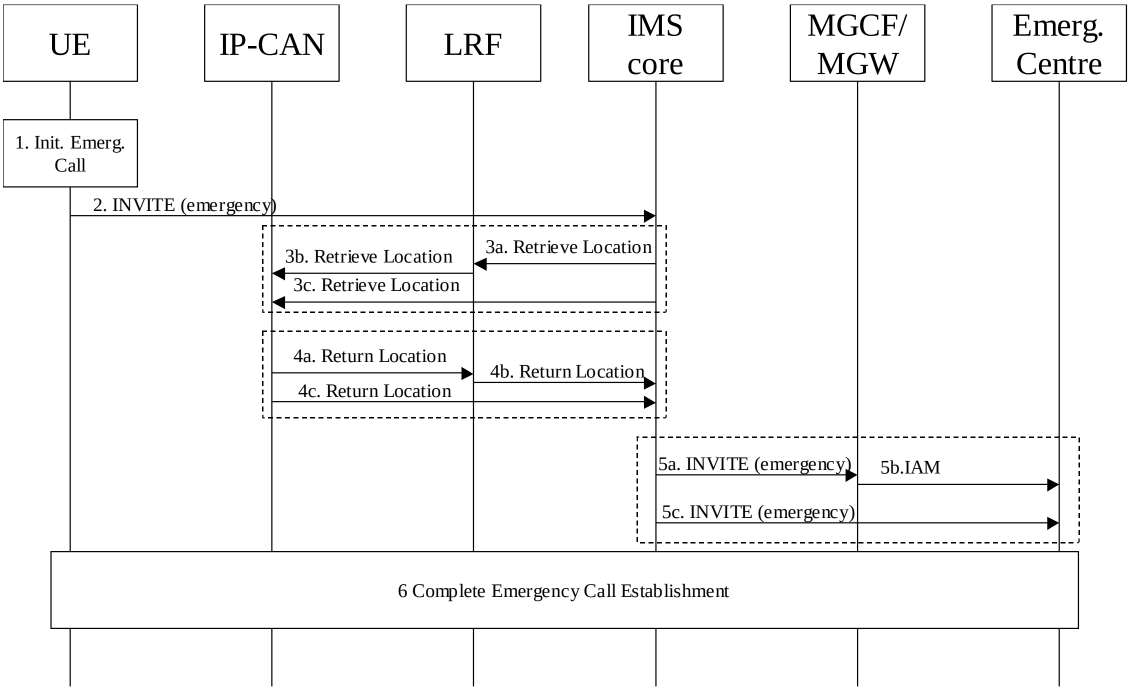

Figure A.2: IMS core requests location information from the LRF

1. The user initiates an emergency call.

2. The user equipment sends an INVITE with an emergency indication to the IMS core.

3. The IMS core requests the location information.
   3a. The retrieve location request is sent to the LRF performing the location retrieval functionality. 3b. The LRF may retrieve location information from the IP-CAN and other databases or has this information already available OR 3c. The Retrieve Location Request is sent directly to the IP-CAN from the IMS core.

4. The representation of the location information is returned to the IMS core.
   4a, 4b. The LRF performing the role of a location retrieval function, returns the location information to the IMS core.
   4c. The IP-CAN returns a representation of the location information to the IMS core.

5. The IMS core selects an emergency centre or PSAP and sends the request including the location information to the emergency centre or PSAP.
   5a. The INVITE is sent to an MGCF/MGW, 5b. The IAM is continued towards the emergency centre or PSAP Or 5c. The INVITE is sent directly to the emergency centre or PSAP.

6. The emergency call establishment is completed.

Annex B: Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2005-09	SP#29	SP-050496	-	-	Revised editorially by MCC for presentation to TSG SA #29 for approval	1.2.0	2.0.0
2005-09	-	-	-	-	Updated by MCC for publication as version 7.0.0	2.0.0	7.0.0
2005-12	SP-30	SP-050803	0002	2	Radio network considerations in case of IMS emergency calls	7.0.0	7.1.0