Technical Specification Group Services and System Aspects
Meeting #28, 06 - 08 June 2005,
Quebec, Canada

TSGS#28(05)0341

Source: **SA WG2**

Title: **CR to TS 23.251: Clarification of PS and CS domain registration coordination (Rel-6)**

Document for: **Approval**

Agenda Item: **7.2.3**

SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers Cur	SA2 Doc	WI	Clauses affected
SP-050341	23.251	0012	4	Rel-6	F	Clarification of PS and CS domain registration coordination	6.3.0	S2-051453	NTShar	4.2.5; 7.1.4

3GPP TSG-SA WG2 Meeting #46
Athens, Greece, 9th - 13th May 2005

Tdoc S2-051453
(S2-051437rev2)

CR-Form-v7

CHANGE REQUEST

⌘	**23.251**	**CR**	**0012**	⌘ **rev**	**4**	⌘	Current version:	**6.3.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☒ Core Network ☒

Title:	⌘	Clarification of PS and CS domain registration coordination
Source:	⌘	SA WG2
Work item code:	⌘	TEI6
Date:	⌘	18/05/2005
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Domain coordination may be done in different ways. The standard only mentions how this is done in Gs enabled networks. It also needs to be specified how to handle this in networks not using the Gs interface.
Summary of change:	⌘	Domain coordination in RNC is described.
Consequences if not approved:	⌘	In absence of Gs interface, PS/CS registration coordination is not possible for UEs roaming from other PLMNs

Clauses affected:	⌘	4.2.5; 7.1.4			
Other specs affected:	⌘	**Y** / **N**	Other core specifications	⌘	25.413
		X /	Test specifications		
		X /	O&M Specifications		
Other comments:	⌘				

First change

4.2.5 PS and CS domain registration coordination

In conventional networks, the same CN operator always serves the UE in CS and PS domains. In a shared network, supporting UEs shall behave as UEs in conventional networks with respect to registration with CS and PS domains. For non-supporting UEs, the Gs interface may be configured to guarantee that the same CN operator serves the subscriber in CS and PS domains.

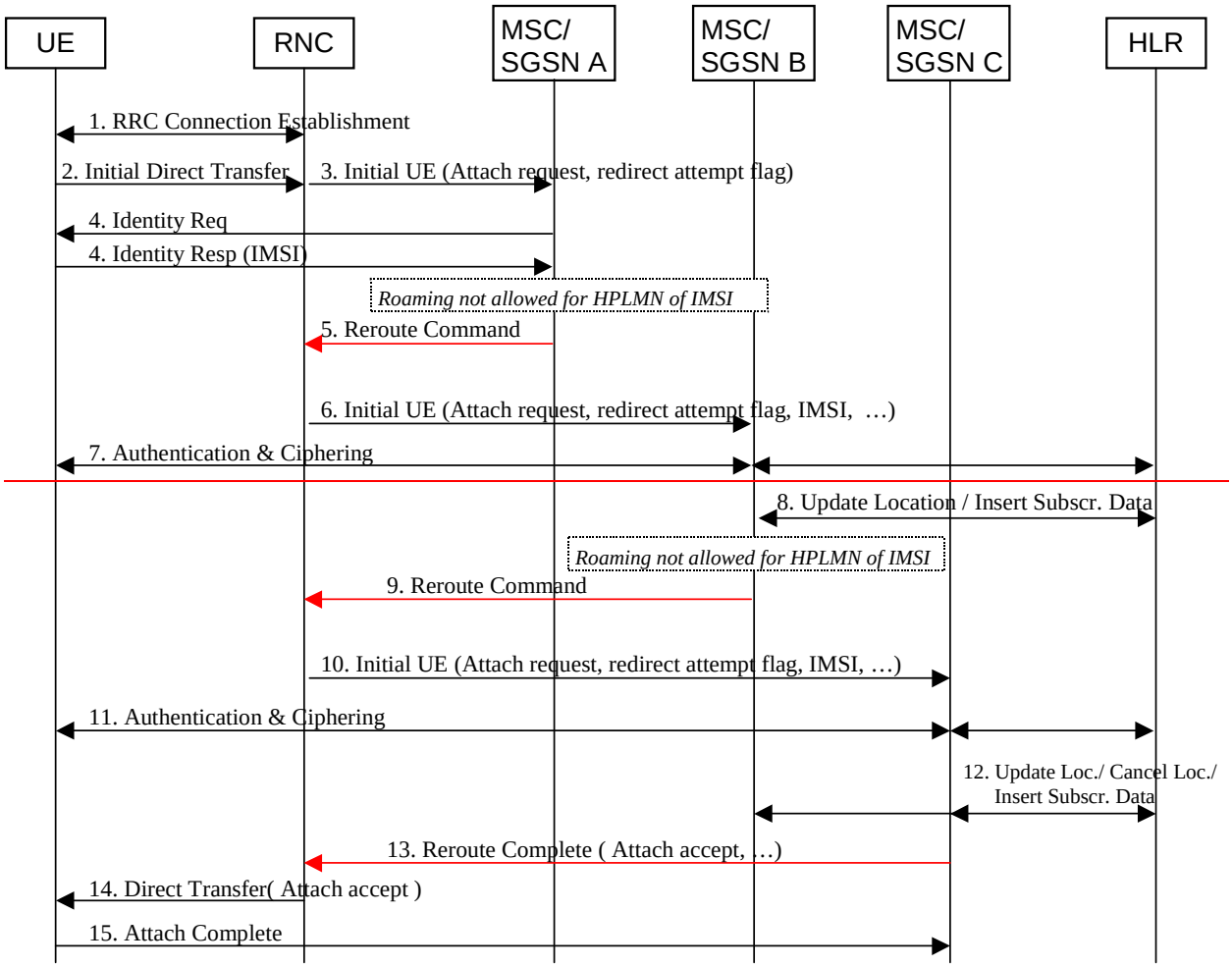
Alternatively, in networks not using Gs the RNC may for non-supporting UE's coordinate that the CS and PS registrations for a given subscriber are always sent to the same CN operator. In that case RNC based coordination of PS and CS domain registration is configured in CN nodes and RNC. When a CN node receives a registration from a subscriber with a non-supporting UE having a P-TMSI/TMSI not belonging to the pool, and no IMSI is provided by RNC, it returns a Reroute Command message to the RNC (according to subclause 7.1.4 "Non-supporting UEs in a MOCN configuration") for coordination purposes. The coordination is done in the RNC (without memorising IMSI information for IDLE mode UEs), e.g.uses a fixed split of IMSI ranges or IMSI hash table between operators. The coordination may result in that the registration is sent back to the same CN node or CN operator again.

A network should not be configured to use RNC coordination when Gs interface is in use.

Next Change

7.1.4 Non-supporting UEs in a MOCN configuration

An example of an information flow for redirection is shown below. In this example an attach request from a non-supporting UE is directed to three different CN operators. The first rejects since it has no roaming agreement with the subscribers Home PLMN. The second rejects because of a roaming restriction found in HLR. The third CN operator accepts and completes the attach request. The different "MSC/SGSNs" in the example below shall be seen as different CN operators. One specific CN operator may also have several pooled MSCs/SGSNs connected to the RNC if Iu-flex is used.


UE
RNC
MSC/ SGSN A
MSC/ SGSN B
MSC/ SGSN C
HLR
1. RRC Connection Establishment
2. Initial Direct Transfer
3. Initial UE (Attach request, redirect attempt flag)
4. Identity Req
4. Identity Resp (IMSI)
Roaming not allowed for HPLMN of IMSI
5. Reroute Command
6. Initial UE (Attach request, redirect attempt flag, IMSI, …)
7. Authentication & Ciphering
8. Update Location / Insert Subscr. Data
Roaming not allowed for HPLMN of IMSI
9. Reroute Command
10. Initial UE (Attach request, redirect attempt flag, IMSI, …)
11. Authentication & Ciphering
12. Update Loc./ Cancel Loc./ Insert Subscr. Data
13. Reroute Complete (Attach accept, …)
14. Direct Transfer(Attach accept)
15. Attach Complete

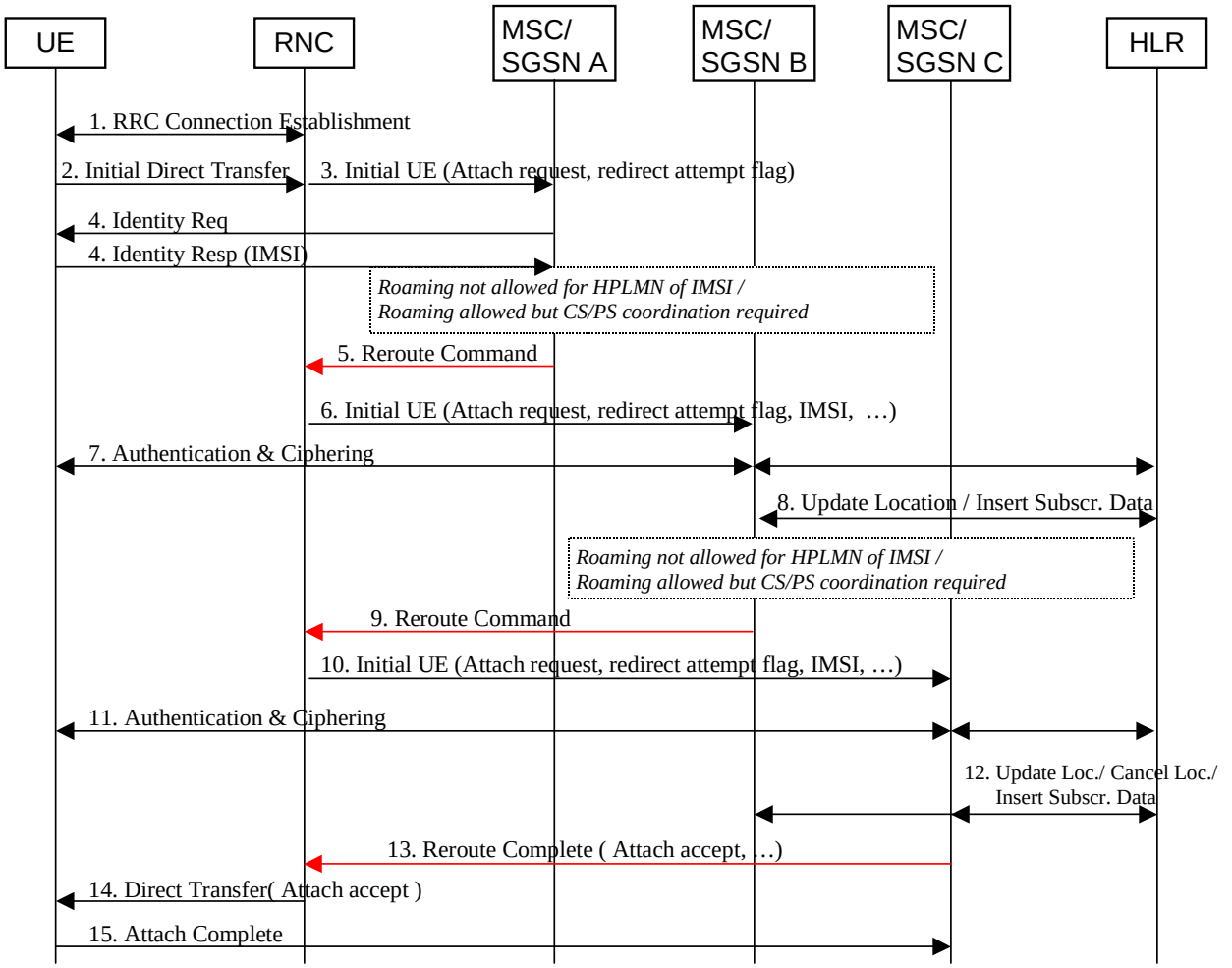


Figure 5: Information flow for redirection.

1) The RRC connection is established.

2) RNC receives an Initial Direct Transfer from an UE. The RNC is configured to work in a Shared RAN MOCN, and therefore it forwards the NAS message in an Initial UE with an additional *redirect attempt flag* set. The flag indicates that the MSC/SGSN shall respond to the attach request with a *Reroute Command* or *Reroute Complete* message. Selection of CN node is based on NRI (valid or invalid) if present in IDNNS or by random selection. A *redirect attempt flag* could also simply be the fact that the Initial UE message does not include any selected PLMN-ID (later RAN3 decision), which a supporting UE would include. Redirect is never done for supporting UEs.

3) The MSC/SGSN receives the Initial UE with the *redirect attempt flag* set. It then knows it shall answer with a *Reroute Command* or *Reroute Complete* message. Those new messages might also be extensions to the Direct Transfer message (later RAN3 decision).

4) The MSC/SGSN needs the IMSI of the UE. It is retrieved either from old MSC / old SGSN or from the UE as in this example. By comparing the IMSI with the roaming agreements of the CN operator, the MSC/SGSN discovers that roaming is not allowed. Attach procedure is aborted.

5) A message is sent back to the RNC with two NAS messages, the attach reject message and the original attach request message received from the UE (alternatively the original NAS message may be stored in the RNC). The IMSI is also included in the message, plus a reject cause code to the RNC. The message should be a new RANAP message, *Reroute Command.* It might also be an extended Direct Transfer message (later RAN3 decision).

The signalling connection between RNC and MSC/SGSN A is released. The RNC selects a MSC/SGSN in the next step. The already tried MSC/SGSNs is stored in the RNC during the redirect procedure so that the same node is not selected twice.

6) The RNC sends a new Initial UE to the next selected MSC/SGSN with the original NAS attach request message. Redirect attempt flag is set and IMSI ~~may~~ shall also be included to avoid a second IMSI retrieval from UE or old MSC/SGSN and to indicate that PS/CS domain coordination has been done in RNC (if enabled in RNC). The MSC/SGSN receiving the message starts its attach procedure.

7) MSC/SGSN B does in general support roaming for the HPLMN of the IMSI and hence authentication is done and RAN ciphering is established.

8) MSC/SGSN B updates the HLR and receives subscriber data from HLR.

9) The subscription data do not allow roaming (e.g. regional or 3G). MSC/SGSN B sends a Reroute Command message including the attach reject message, a reject cause code, the original attach request message (alternatively stored in the RNC), and the N(SD) (for MSC only). IMSI is included in Reroute Command message only if it was not included in the Initial UE received by the MSC/SGSN.

   The signalling connection between the RNC and the MSC/SGSN B is released. The RNC then selects a new MSC/SGSN as in step 5.

10) The MSC/SGSN **C** receives an Initial UE (with the original NAS attach request message) with the redirect attempt flag is set, an IMSI, and N(SD) (if MSC). The MSC/SGSN C starts the attach procedure and uses provided information (IMSI and N(SD)).

11) MSC/SGSN C does in general support roaming for the HPLMN of the IMSI and hence authentication is done and RAN ciphering is established.

12) MSC/SGSN C updates the HLR and receives subscriber data from HLR. Subscriber data allows roaming, and the MSC/SGSN C completes the attach procedure. This includes the assignment of a new TMSI/P-TMSI with an NRI that can be used by RNC to route subsequent signalling between UE and correct MSC/SGSN (Iu-flex functionality). The Update Location sent to HLR also triggers a Cancel Location sent to the MSC/SGSN B.

13) A *Reroute Complete* message with the NAS Attach accept message is sent to RNC. By usage of a specific Reroute Complete message, the RNC knows that the redirect is finished and can both forward the NAS message to the UE and clean up any stored redirect data (it is a later RAN3 decision if an extension to the Direct Transfer message shall be used instead of a new message).

14) The Attach Accept is forwarded to the UE. The UE stores the TMSI/P-TMSI with the Iu-flex NRI to be used for future signalling, even after power off. This is existing functionality.

15) UE responds with an Attach Complete message.

If the RNC finds no more MSC/SGSN to redirect to after receiving a Reroute Command message, e.g. step 5 or step 9, it compares the cause code with cause codes from other Reroute Command messages it has earlier received for this UE. A cause code ranking is done and the "softest" cause code is chosen and the corresponding saved NAS attach reject message is returned to the UE.

Each CN node that receives an Initial UE, shall run its own authentication procedure. This may in some rare situations cause the UE to be authenticated more than once, however the trust-model used is that one CN operator shall not trust an authentication done by another CN operator. This will of course not be an optimal usage of radio resources, but given the rare occurrence of this, the increased signalling should not be of any significance.

During the redirect procedure the RNC keeps a timer, which corresponds to the UE timer of releasing the RR connection (20 seconds). If the RNC when receiving a Reroute Command message finds that there is not sufficient time for another redirect, further redirect attempts are stopped (for this attach request message). The UE will repeat its attach request four times (each time waiting 15 seconds before it re-establishes the RR connection for another try).

End of changes