Technical Specification Group Services and System Aspects **TSGS#24(04)0324**
Meeting #24, Seoul, Korea 7-10 June 2004

Source: **TSG SA WG2**
Title: **CRs on 23.851 (Network Sharing)**
Agenda Item: **7.2.3**

The following Change Requests (CRs) have been approved by TSG SA WG2 and are requested to be approved by TSG SA plenary #24.
Note: the source of all these CRs is now S2, even if the name of the originating company(ies) is still reflected on the cover page of all the attached CRs.

S2 doc #	Title	Spec	CR #	cat	Version in	REL	WI	S2 meeting	Clauses affected
S2-042337	Clarification of Gs usage	23.851	001r1	F	6.0.0	6	Netshar	S2 #40	4.6
S2-041434	Clarification of CN operator identity usage in MSC and SGSN	23.851	005r1	F	6.0.0	6	Netshar	S2 #39	5.4, 5.5
S2-042327	Information flow of the CN centric redirection	23.851	006r4	F	6.0.0	6	NTShar	S2 #40	4.3
S2-042323	Detailing RAN Centric redirection	23.851	011r3	F	6.0.0	6	NTShar	S2 #40	4.3
S2-042325	Connection-less interrogation as optimisation	23.851	012r3	F	6.0.0	6	NTShar	S2 #40	4.3.z

3GPP TSG-SA2 Meeting #40 **S2-042337**
Sophia Antipolis, 17-21 May, 2004

CR-Form-v7

CHANGE REQUEST

⌘ **23.851** **CR** **001** ⌘ **rev** **1** ⌘ Current version: **6.0.0** ⌘

*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 **X**

Title:	⌘	Clarification of Gs usage
Source:	⌘	Nortel Networks
Work item code:	⌘	NTShar
Date:	⌘	19/04/2004
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:	⌘	The current TR indicates that "Supporting UEs should select the same CN operator for CS and PS domains". With this behaviour, a UE will always be attached to the same Operator for PS and CS domain. There is no need of Gs interface to ensure this for supporting UEs while this is indicated currently as FFS in the TR: "to ensure or support the selection of the same operator for both domains FFS".
Summary of change:	⌘	Remove this last FFS sentence.
Consequences if not approved:	⌘	Gs seems to be mandated for supporting UEs.

Clauses affected:	⌘	4.6

Other specs affected: ⌘	Y	N		⌘
		X	Other core specifications	
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘ .

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

4.6 Usage of Gs interface

[Editor's note: It seems that multi-operator CN has certain impacts to the usage of Gs interface. Currently only one network mode of operation can be broadcast over the radio interface whereas in multi-operator CN operators may have different network configurations. The problem and the principle of the associated solution is described here.]

In networks without network sharing a UE is always served by the same CN operator for PS and CS domains. This behaviour should continue in networks that are shared.

The Gs interface may be configured to guarantee that the same CN operator serves the subscriber in CS and PS domains for non-supporting UEs. For GWCN the Gs messages indicate the CN operator that serves already the PS domain to the CS domain. For MOCN it is sufficient to configure the Gs interface as for this scenario the Gs is configured only between nodes belonging to the same CN operator.

Supporting UEs should select the same CN operator for CS and PS domains. The Gs interface may be used to reduce the time until a UE is attached to CS and PS domains ~~and to ensure or support the selection of the same operator for both domains. FFS~~.

3GPP TSG-SA WG2 Meeting #39
Shenzhen, China, 19th - 23rd April 2004.

Tdoc ⌘S2-041434

CR-Form-v7

CHANGE REQUEST

⌘ **23.851** **CR** **005** ⌘ **rev** **1** ⌘ Current version: **6.0.0** ⌘

*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 **X**

Title:	⌘	Clarification of CN operator identity usage in MSC and SGSN
Source:	⌘	SA2 (Ericsson)
Work item code:	⌘	Netshar
Date:	⌘	21/04/2004
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:	⌘	Unclear usage of parameter in MSC and SGSN.
Summary of change:	⌘	Usage has been clarified.
Consequences if not approved:	⌘	Misinterpretations of Netshare TR.

Clauses affected:	⌘	5.4, 5.5

	Y	N		
Other specs affected: ⌘		X	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

5.4 MSC Functions

When a UE accesses the MSC the first time, i.e. when there is no VLR entry for this UE, the MSC verifies whether the UE belongs to one of the operators sharing the MSC or their roaming partners. For that purposes the MSC derives the IMSI from another MSC/VLR or from the UE. In case of GWCN the MSC determines a serving CN operator unless the old MSC/VLR or the UE have indicated a CN operator. For GWCN the MSC/VLR stores the serving CN operator, for the sole purpose of separating. The serving CN operator attribute is then only used to separate charging information for different CN operators (see subclause 6.2). In case of MOCN or when Iu-Flexibility [8] is configured together with GWCN the MSC may need to transfer the UE to another MSC, for example, when the MSC does not belong to the selected operator or for load balancing between MSCs serving the same shared network area by means of Iu-Flexibility. In case of MOCN or when Iu-Flexibility [8] is configured together with GWCN the MSC/VLR that finally serves the UE assigns to the UE a Network Resource Identifier, which is part of the TMSI. All subsequent UE accesses the RAN routes to the serving MSC/VLR.

5.4.1 Transferring UEs to another MSC/VLR

If the first MSC is not able to provide service to the UE, the MSC needs to be able to transfer the UE to another CN. Mechanisms for this and related MSC functions are described in “Assignment of CN operator and CN node”.

5.5 SGSN Functions

When a UE accesses the SGSN the first time, i.e. when the UE is not yet known by the SGSN, the SGSN verifies whether the UE belongs to one of the operators sharing the SGSN or their roaming partners. For that purposes the SGSN derives the IMSI from another SGSN or from the UE. In case of GWCN the SGSN determines a serving CN operator unless the old SGSN or the UE have indicated a CN operator. For GWCN the SGSN stores the serving CN operator, for the sole purpose of separating. The serving CN operator attribute is then only used to separate charging information for different CN operators (see subclause 6.2). In case of MOCN or when Iu-Flexibility [8] is configured together with GWCN the SGSN may need to transfer the UE to another SGSN, for example, when the SGSN does not belong to the selected operator or for load balancing between SGSNs serving the same shared network area by means of Iu-Flexibility. In case of MOCN or when Iu-Flexibility [8] is configured together with GWCN the SGSN that finally serves the UE assigns to the UE a Network Resource Identifier, which is part of the TMSI. All subsequent UE accesses the RAN routes to the serving SGSN.

5.5.1 Transferring UEs to another SGSN

If the first SGSN is not able to provide service to the UE, the SGSN needs to be able to transfer the UE to another CN. Mechanisms for this and related SGSN functions are described in “Assignment of CN operator and CN node”.

6 Charging and Accounting Aspects

In [6] it is stated that charging solutions shall support the shared network architecture so that both end users and network sharing partners can be correctly charged for their usage of the shared network.

6.1 Inter-operator charging and accounting

CN operators will presumably consume different amount of resources of the shared RAN. The RAN operator may therefore want to charge CN operators accordingly. Generally, volume/time based charging and accounting will not be sufficient because resource consumption is also dependent on quality parameters (e.g. Eb/No - power consumption) of the delivered resources. It is FFS whether the shared RNS therefore should be capable of generating the following charging and accounting information:

- Identity of CN Operator (probably PLMN-id), whose end user has consumed the resource of the RAN.
- Resource, e.g. radio bearer
- Start time – indicating the set up time of radio resource.

- op time – indicating the time the radio resource was released.
- ference to geographical area where the radio resource was used, e.g. cell reference.
- SI of the end user, who has consumed radio resource.

It is noted that the information generated in the RNS is not intended for end-user charging. The format of the charging information ("RAN-CDR") should be standardized.

[Editor's note: It might be possible to provide this charging information by monitoring the Iu interface signalling. This needs further study, but solutions that minimise the impact on the RNC are desirable.]

6.2 End customer charging

End users should be correctly charged in a shared network. The charging system of the shared network should be able to separate the charging information generated by shared MSC/SGSN and send it to the correct CN operator, i.e. the CN operator that served the end user, based on available information in the CDRs generated by the shared MSC/SGSN.

Note: This section is only relevant in the GWCN, where MSC/SGSNs are shared.

3GPP TSG-SA2 Meeting #40 ***S2-042327***
Sophia Antipolis, 17-21 May, 2004 rev of S2-041683 and S2-041993

CR-Form-v7

CHANGE REQUEST

⌘ **23.851** **CR** **006** ⌘ **rev** **4** ⌘ Current version: **6.0.0** ⌘

*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:	⌘	Information flow of the CN centric redirection
Source:	⌘	SA2 (Siemens)
Work item code:	⌘	NTShar
Date:	⌘	21/05/2004
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:	⌘	The current TR does not contain any information flows for the redirection of UEs between CN operators in MOCN configurations. An information flow is added for a better description of the mechanims.
Summary of change:	⌘	Clarifications for the CN centric redirection of UEs between CNs.
Consequences if not approved:	⌘	There are different interpretations of the CN centric redirection possible.

Clauses affected:	⌘	4.3			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘	.			

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

4.3 Assignment of CN operator and CN node

4.3.1 Description

In case of MOCN the redirection to another CN operator requires a change of the CN node until a CN node is found that serves the UE. Possible mechanisms to do this are:

1. The CN node may indicate to RNC that the initial NAS message should be forwarded to a node of another CN operator. Other information, like current value of N(SD), subscriber's identity (IMSI), unused authentication vectors, and 'list of already tried PLMN IDs ' may be forwarded too. The following mechanisms for handling of the redirection in the RNC have been identified:

    a. The RNC keeps track of what CN operators has been tried during the assignment procedure. This can be done either through a 'list of already tried PLMN IDs' that is sent back and forth to the CN operators' nodes or through an information kept in the RNC during the assignment procedure. It is ffs which of these two methods is the best.

    b. Redirecting in RNC based on a random or weighted random selection to one of the remaining CN operators may be done. This ensures a statistical distribution between the available CN operators.

    c. Redirecting in RNC based on the IMSI passed from the CN node may be done. The IMSI analysis may be simple e.g. only recognizing IMSI's of the CN operators of the MOCN, or may be more extensive based on roaming agreement information of the sharing CN operators configured into the RNC. To what extent IMSI analysis is done may be implementation specific.

    d. Preventing the UE from timing out during the assignment procedure may be handled by counting the number of redirects or measuring the time duration of the assignment procedure. If a redirect limit or time limit is passed when the RNC receives a new redirect request from a CN node, the RNC may simply drop the whole registration message. The UE is then expected to resend the registration request. If the redirect counter or redirect timer is kept in RNC or passed back and forth between the CN operators' nodes is ffs.

    e. The setting of an appropriate cause code in the NAS registration reject message if all CN operators has rejected before redirect count limit or redirect timeout must be handled. This may include solutions such as never returning any NAS registration reject message to the UE, a cause code ranking in the RNC and modification of the cause code in the NAS reject message by the RNC, or any other more or less advanced setting of the cause code in collaboration between RNC and CN-nodes. The solution for how to handle the setting of the cause code is ffs.

2. The CN node may ask a node of another CN operator to serve the UE. The CN node, which will be able to serve the UE, allocates a Network Resource Identity to the UE. At the next NAS establishment, after this TMSI and Network Resource Identity allocation by the second CN, the signalling goes directly between UE and second CN node. There are two options envisaged for this:

    a. The first CN node asks other CN nodes of other operator(s) whether they want to serve the UE. It selects one CN node which has accepted to serve the UE and allocates to the UE an NRI received from the selected CN node. The selected CN node may also provide the first CN node with information to authenticate the UE. Information flows are described below in subclause 4.3.2.

    b. The first CN node forwards the initial NAS message to a second CN of another operator that might serve the UE, and then relays the L3 signalling between UE and second CN node.

3. The first CN node allocates a Network Resource Identity from a CN node of another operator to the UE and a 'wrong' LA/RA. This causes the UE to re-attach to another operator's CN node, which might serve the UE. For that purpose a range of NRIs from other CN nodes is configured on the first CN node.

All methods could present an issue with the MM timers in the UE if the redirect takes too long time. Method 1 requires some Iu, A and Gb enhancements. The method transfers the parts of or the complete (G)MM protocol machine possibly including link layer status from one CN node to another. It is ffs what information needs to be transferred. The handling for method 1 may involve several or all of the alternatives a) to e) above.

Method 2 requires some inter SGSN and inter MSC signaling enhancements. Method 2 works in A/Gb mode as well as in Iu mode.

Method 3 requires each CN node to derive authentication vectors from HLRs of networks that are not served by the CN node as the TMSI that contains the Network Resource Identity is allocated encrypted only. When multiple CN operators share the network this may require multiple attach/update procedures. The UE may receive services first when an update/attach is accepted by a serving CN node.

When a UE performs an initial access to a shared network one of available CN operators is selected to serve the UE. If due to Iu-Flexibility [8] multiple CN nodes of the selected CN operator serve the UE's location then one from these CN nodes is selected to serve the UE. After this initial access to the shared network the UE does not change to another available CN operator as long as the selected CN operator is available to serve the UE's location. Only the network selection procedures specified in 23.122 may cause a reselection of another available CN operator. Furthermore the UE does not change to another CN node as long as the selected CN node is available to serve the UE's location. The mechanisms specified for Iu-Flexibility [8] manage that CN operator and CN node are not changed as long as CN operator and CN node can serve the UE's location.

The RAN routes the UE's initial access to a shared network to one of the available CN nodes. For non-supporting UEs the shared network selects an operator from the available CN operators. Supporting UEs may select an operator from the available CN operators. When MOCN or when Iu-Flexibility [8] are configured it may be necessary to transfer the UE's initial access from one CN node to another, e.g. as the accessed CN node does not belong to the selected operator or because of load balancing between CN nodes belonging to the selected operator.

When MOCN or when Iu-Flexibility [8] are configured and the UE's initial access to the shared network is confirmed by the CN node of the selected CN operator the UE gets assigned a Network Resource Identifier as defined for Iu-Flexibility [8] and all subsequent accesses to the shared network the RAN routes to the serving CN node of the serving CN operator.

4.3.2 Information flow for CN centric redirection

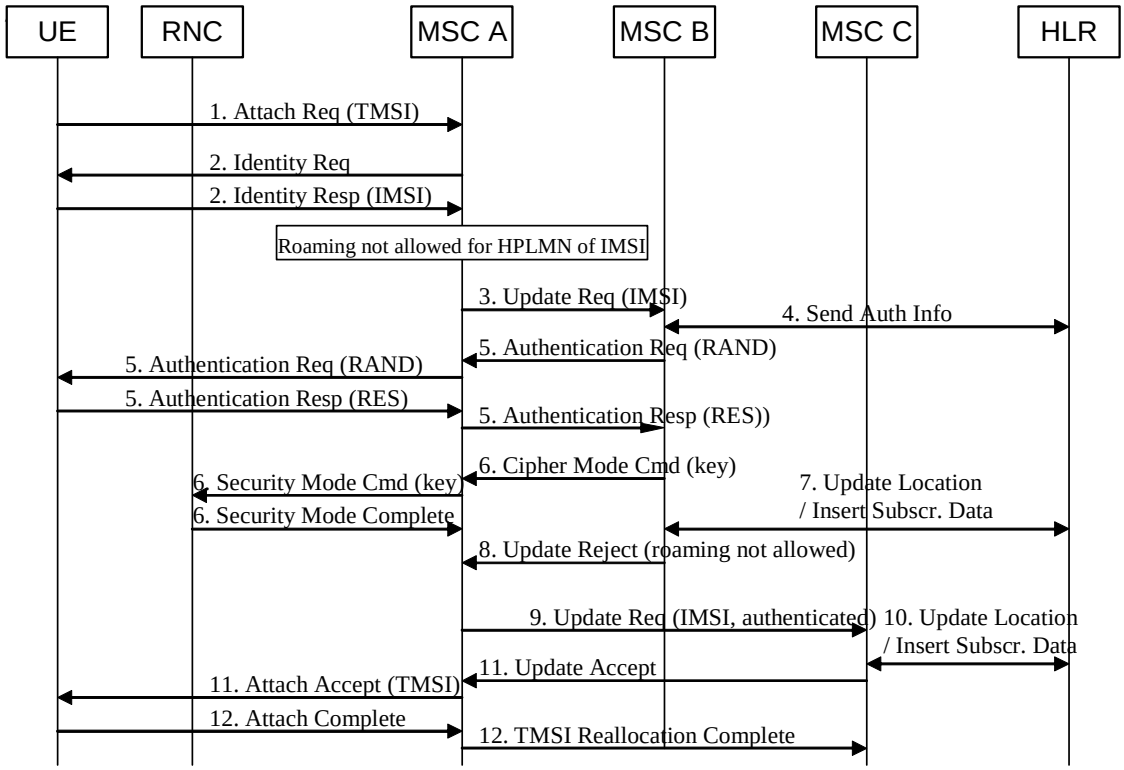

Figure 6: Information flow for CN centric redirection with connection-oriented signalling.

1) The UE selected the shared RAN and sends an Attach Request with TMSI. The RAN routes the signalling based on the NRI to MSC A. Or, if there is no CN node configured in RAN for the indicated NRI the RAN selects a CN node by load balancing or other rules.

2) When MSC A can not resolve the TMSI, MSC A performs the Identity Request procedure to get the IMSI from the UE. There is no need to contact MSCs of other operators as the NRI value space is coordinated between sharing CN operators and the first message is already routed to the CN operator that uses the UE's NRI. This assumes that also non-shared networks like GERAN networks which sharing CN operators use in parallel to the shared network use the same NRI split. Otherwise, first all other CNs need to try to resolve the TMSI.

3) MSC A determines from the IMSI that roaming is not allowed for the subscriber. MSC A selects the next MSC to which attachment should be tried and sends an Update Request to this MSC (MSC B). This message is sent on a signalling connection that the RNC provides between the two MSCs in which RNC routing does not require to store any MM UE information during the assignment procedure.

4) MSC B supports in general roaming for the HPLMN of the IMSI and requests Authentication Vectors from the HLR.

5) MSC B asks MSC A to authenticate the subscriber.

6) MSC B compares the authentication result and asks MSC A to start RAN ciphering.

7) MSC B updates the HLR and receives subscriber data from HLR.

8) The subscription data do not allow (e.g. regional or 3G) roaming. MSC B sends a reject message to MSC A. The signalling connection between the MSCs is released.

9) MSC A selects another MSC to which attachment should be tried, sends another Update Request to this MSC (MSC C) and indicates that the UE is already authenticated and that ciphering started. This message is sent on a signalling connection that the RNC provides between the two MSCs.

10) MSC C updates the HLR and receives subscriber data from HLR.

11) Subscriber data allow for roaming and MSC C ask MSC A to accept the attach request and to allocate the new TMSI to the UE.

12) The UE confirms the new TMSI with Attach Complete, which MSC A indicates to MSC C.

13) As the attach is performed via another MSC a potential follow on proceed request is ignored and the signalling connection with the UE is released.

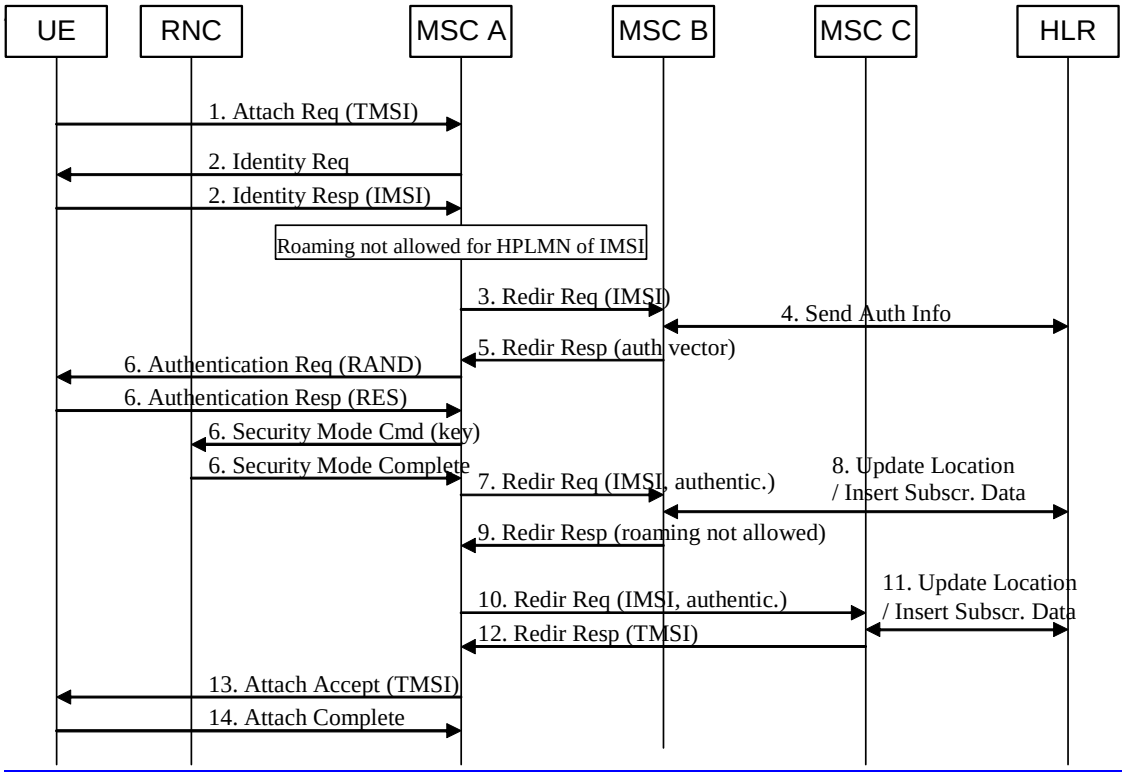

Figure 7: Information flow for connection-less CN centric redirection.

1) The UE selected the shared RAN and sends an Attach Request with TMSI. The RAN routes the signalling based on the NRI to MSC A. Or, if there is no CN node configured in RAN for the indicated NRI the RAN selects a CN node by load balancing or other rules.

2) When MSC A can not resolve the TMSI it may perform redirection requests with the TMSI instead with the IMSI. Otherwise, MSC A performs the Identity Request procedure to get the IMSI from the UE. When the NRI value space is coordinated between sharing CN operators then MSCs don't need to contact MSCs of other operators as the first message is already routed to the CN operator that uses the UE's NRI. This assumes that also non-shared networks like GERAN networks which sharing CN operators use in parallel to the shared network use the same NRI split. Otherwise, first all other CNs need to try to resolve the TMSI.

3) MSC A determines from the IMSI that roaming is not allowed for the subscriber. MSC A sends an Redirection Request to the RNC. Together with the Redirection Request it is indicated that redirection is required and a bitmap information element is added to keep track on redirections. The RNC determines a redirection target (MSC B in this case), marks CN B in the bitmap and forwards the Redirection Request together with the bitmap to MSC B. This message is sent connection-less on signalling resources that the RNC provides between the two MSCs The RNC does not store any UE specific information during the redirection.

4) MSC B supports in general roaming for the HPLMN of the IMSI and requests Authentication Vectors from the HLR.

5) MSC B provides an authentication vector to MSC A and returns also the bitmap.

6) MSC A authenticates the UE and starts RAN ciphering.

7) MSC A sends another Redirection Request to the RNC together with the bitmap. The RNC forwards the message to MSC B. The message indicates that the IMSI is authenticated.

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

9) The subscription data do not allow roaming (e.g. regional or 3G restrictions). MSC B sends a Redirection Response message to MSC A indicating a reject cause "roaming not allowed".

10) MSC A sends again Redirect Request together with the bitmap and the indication that redirection is required to trhe RNC. The RNC determines a redirection target (MSC C in this case), marks CN C in the bitmap and forwards the Redirection Request together with the bitmap to MSC C. The message indicates that the IMSI is authenticated.

11) MSC C updates the HLR and receives subscriber data from HLR.

12) Subscriber data allow for roaming and MSC C allocates a TMSI for the UE and sends it in the Redirection Response message to MSC A.

13) MSC A accepts the Attach and sends the new TMSI to the UE.

14) The UE confirms the new TMSI with Attach Complete.

After attach the signalling connection between UE and MSC A is released. Any subsequent mobile originated or mobile terminated transaction is routed to MSC C because of the allocated NRI. At the first signalling connection between UE and MSC C the UE may be re-authenticated and the TMSI may be reallocated.

MSC A repeats the redirection procedure until another MSC delivers a TMSI, or until the RNC rejects the redirection request, which indicates that no more CNs are available for redirection. This RNC reject indicates whether all CNs are tried, which causes a reject to the UE with “PLMN not allowed”, or whether additional CNs are available in other parts of the shared RAN, which causes a reject to the UE with “no suitable cell in LA”.

Alternatively this mechanism may use connection-oriented signalling.

3GPP TSG-SA WG2 Meeting #40 **Tdoc ⌘S2-042323**
Sophia Antipolis, France, 17th – 21st May 2004

CR-Form-v7

CHANGE REQUEST

⌘ **23.851** **CR** **11** ⌘ **rev** **3** ⌘ Current version: **6.0.0** ⌘

*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:	⌘	Detailing RAN Centric redirection			
Source:	⌘	SA2 (Ericsson, TeliaSonera)			
Work item code:	⌘	Netshar	***Date:*** ⌘	19/05/2005	
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:	⌘	The RAN Centric approach for redirection needs detailing and removal of FFS'es
Summary of change:	⌘	Removal of FFS'es and clarifications in subclause 4.3 and additional of a new subclause with an example of information flow for a RAN Centric redirection.
Consequences if not approved:	⌘	Unclear description.

Clauses affected:	⌘	4.3			
Other specs Affected:	⌘	Y / N	Other core specifications	⌘	
		☐ / ☒	Test specifications		
		☐ / ☒	O&M Specifications		
Other comments:	⌘				

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

4.3 Assignment of CN operator and CN node

In case of MOCN the redirection to another CN operator requires a change of the CN node until a CN node is found that serves the UE. Possible mechanisms to do this are:

1. The CN node may indicate to RNC that the initial NAS message should be forwarded to a node of another CN operator. Other information, like current value of N(SD), subscriber's identity (IMSI), ~~unused authentication vectors,~~ and cause code ~~'list of already tried PLMN IDs '~~ may be forwarded too. The following mechanisms for handling of the redirection in the RNC have been identified (in subclause 4.x below is an information flow also given):

   a. The RNC keeps track of what CN operators ~~has~~ have been tried during the assignment procedure. ~~This can be done either through a 'list of already tried PLMN IDs' that is sent back and forth to the CN operators' nodes or~~ It is done through ~~an~~ information kept in the RNC during the assignment procedure. ~~It is ffs which of these two methods is the best.~~

   b. Redirecting in RNC based on a random or weighted random selection to one of the remaining CN operators may be done. This ensures a statistical distribution between the available CN operators.

   c. As an optimization, r~~R~~edirecting in RNC based on the IMSI passed from the CN node may be done. ~~The~~ Only IMSI ranges of ~~analysis may be simple e.g. only recognizing IMSI's of~~ the CN operators of the MOCN are ~~, or may be more extensive based on roaming agreement information of the sharing CN operators~~ configured into the RNC. The gain from using this optimization in relation to complexity in the network is FFS.~~To what extent IMSI analysis is done may be implementation specific.~~

   d. Preventing the UE from timing out during the assignment procedure ~~may be~~is handled by ~~counting the number of redirects or~~ measuring the time duration of the assignment procedure. If ~~a redirect limit or time limit is passed~~there is not sufficient time to do a new attach attempt, ~~when the RNC receives a new redirect request from a CN node,~~ the RNC ~~may~~ simply drops the whole registration message. The UE is then expected to resend the registration request. ~~If the redirect counter or redirect timer is kept in RNC or passed back and forth between the CN operators' nodes is ffs.~~

   e. The setting of an appropriate cause code in the NAS registration reject message if all CN operators has rejected ~~before redirect count limit or redirect timeout must be~~should be handled by RNC. ~~This may include solutions such as never returning any NAS registration reject message to the UE, a~~The RNC does a cause code ranking and returns the corresponding ~~in the RNC and modification of the cause code in the~~ NAS reject message to the UE. Information stored in a cache is used.

   ~~by the RNC, or any other more or less advanced setting of the cause code in collaboration between RNC and CN nodes. The solution for how to handle the setting of the cause code is ffs.~~

   f. As an optimization, the connection-less interrogation described below may be considered. The gain from using this optimization in relation to complexity in the network is FFS.

2. The CN node may ask a node of another CN operator to serve the UE. The CN node, which will be able to serve the UE, allocates a Network Resource Identity to the UE. At the next NAS establishment, after this TMSI and Network Resource Identity allocation by the second CN, the signalling goes directly between UE and second CN node. There are two options envisaged for this:

   a. The first CN node asks other CN nodes of other operator(s) whether they want to serve the UE. It selects one CN node which has accepted to serve the UE and allocates to the UE an NRI received from the selected CN node. The selected CN node may also provide the first CN node with information to authenticate the UE.

   b. The first CN node forwards the initial NAS message to a second CN of another operator that might serve the UE, and then relays the L3 signalling between UE and second CN node.

3. The first CN node allocates a Network Resource Identity from a CN node of another operator to the UE and a 'wrong' LA/RA. This causes the UE to re-attach to another operator's CN node, which might serve the UE. For that purpose a range of NRIs from other CN nodes is configured on the first CN node.

All methods could present an issue with the MM timers in the UE if the redirect takes too long time. Method 1 requires some Iu, A and Gb enhancements. The method transfers the parts of or the complete (G)MM protocol machine possibly including link layer status from one CN node to another. It is ffs what information needs to be transferred. The handling for method 1 may involve several or all of the alternatives a) to ~~e~~f) above.

Method 2 requires some inter SGSN and inter MSC signaling enhancements. Method 2 works in A/Gb mode as well as in Iu mode.

Method 3 requires each CN node to derive authentication vectors from HLRs of networks that are not served by the CN node as the TMSI that contains the Network Resource Identity is allocated encrypted only. When multiple CN operators share the network this may require multiple attach/update procedures. The UE may receive services first when an update/attach is accepted by a serving CN node.

When a UE performs an initial access to a shared network one of available CN operators is selected to serve the UE. If due to Iu-Flexibility [8] multiple CN nodes of the selected CN operator serve the UE's location then one from these CN nodes is selected to serve the UE. After this initial access to the shared network the UE does not change to another available CN operator as long as the selected CN operator is available to serve the UE's location. Only the network selection procedures specified in 23.122 may cause a reselection of another available CN operator. Furthermore the UE does not change to another CN node as long as the selected CN node is available to serve the UE's location. The mechanisms specified for Iu-Flexibility [8] manage that CN operator and CN node are not changed as long as CN operator and CN node can serve the UE's location.

The RAN routes the UE's initial access to a shared network to one of the available CN nodes. For non-supporting UEs the shared network selects an operator from the available CN operators. Supporting UEs may select an operator from the available CN operators. When MOCN or when Iu-Flexibility [8] are configured it may be necessary to transfer the UE's initial access from one CN node to another, e.g. as the accessed CN node does not belong to the selected operator or because of load balancing between CN nodes belonging to the selected operator.

When MOCN or when Iu-Flexibility [8] are configured and the UE's initial access to the shared network is confirmed by the CN node of the selected CN operator the UE gets assigned a Network Resource Identifier as defined for Iu-Flexibility [8] and all subsequent accesses to the shared network the RAN routes to the serving CN node of the serving CN operator.

4.x Information flow for RAN centric redirection

An example of an information flow for the RAN centric 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 of course also have several pooled MSCs/SGSNs connected to the RNC if Iu-flex is used. This is discussed further in subclause 4.y.

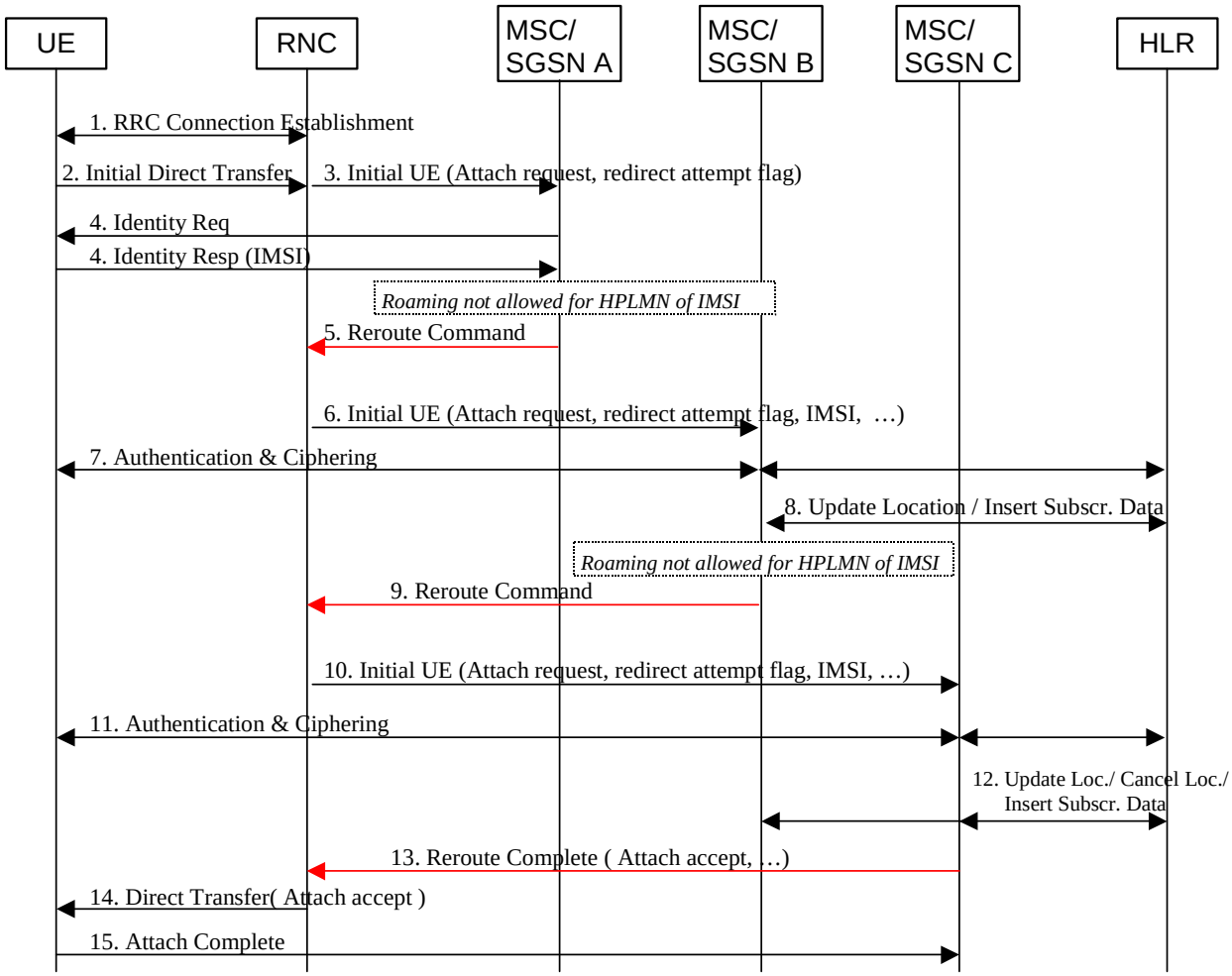

***Figure X**, Information flow for RAN centric redirection*

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 also be included to avoid a second IMSI retrieval from UE or old MSC/SGSN. 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). The risk that a random selection after four retries would still have missed one MSC/SGSN that would have accepted the UE can be calculated to a very small probability.

4.y RAN Centric redirection architectural description aspects

- The used IMSI ranges of all the CN operators in the shared network may be configured in each RNC in shared RAN. This ensures that never more than one redirection is needed for home subscribers of the CN operators of the shared network.

- Specification and design of the redirect function must consider that a CN operator shall be able to use pooled CN resources, i.e. Iu-flex. Moreover, the redirect selection function (using stored info in RNC e.g. earlier tried nodes, info received in Reroute Command and randomising function) is highly related to the Iu-flex selection function in the RNC, see figure below. This needs to be considered when specifying the redirect function to minimize impact in standards and products.

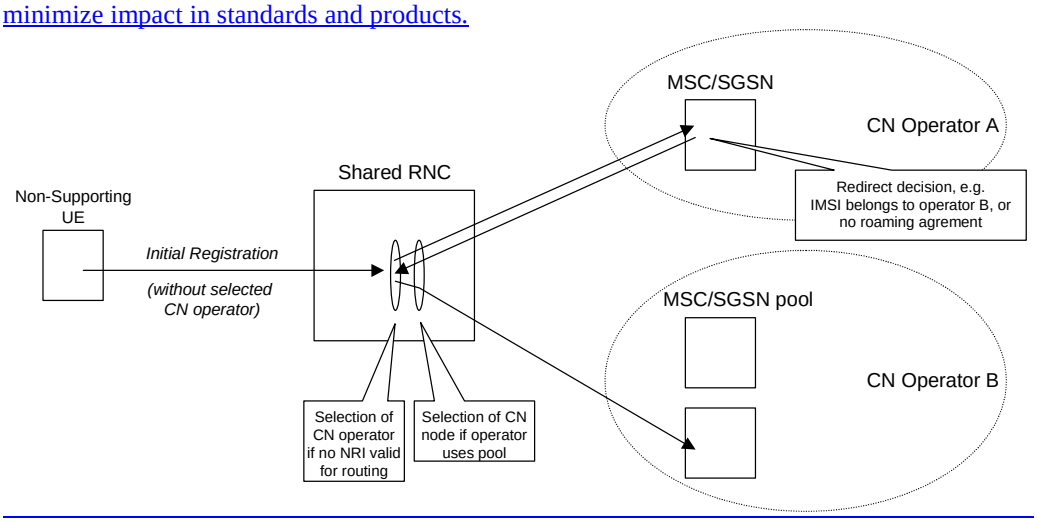

***Figure Y**, Pool aspects for MOCN redirect function*

- There may be need for special consideration to be taken when the coverage of the shared RAN is non-coinciding for all the CN operators.

3GPP TSG-SA WG2 Meeting #40 *Tdoc ⌘S2-042325*
Sophia Antipolis, France, 17th – 21st May 2004

CR-Form-v7

CHANGE REQUEST

⌘ **23.851** **CR** **012** ⌘ **rev** **3** ⌘ Current version: **6.0.0** ⌘

*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:	⌘	Connection-less interrogation as optimization
Source:	⌘	SA2 (Ericsson, Nortel)
Work item code:	⌘	Netshar
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:	⌘	Connection-less interrogation may be done in different ways. The way it is done in this CR is as an overlay procedure which in some MOCN configurations may optimise the response time. It is estimated that when the MOCN has more than three sharing CN operators, the connection-less interrogation will be an optimisation and allow a better handling of the redirect procedure.
Summary of change:	⌘	A new subclause 4.3.z is added describing the additions and changes of the RAN centric redirect procedure.
Consequences if not approved:	⌘	The possibility to optimise the redirect procedure for large shared networks is lost.

Clauses affected:	⌘	4.3.z

Other specs affected: ⌘	Y	N		⌘
		X	Other core specifications	
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

4.3.z Connection-less interrogation in RAN Centric redirection

To optimise the response time for attach of non-supporting UEs without valid NRI in larger shared networks, a connection-less interrogation of CN nodes may be used. In smaller shared networks, a longer response time may result from performing a connection-less interrogation. The gain from the connection-less interrogation in relation to complexity in the network is FFS.

The connection-less interrogation is an optimisation in the RAN centric redirect procedure and is described in the information flow diagram below. The connection-less interrogation provides a preliminary answer to the question if the CN operator can accept an attach from the UE. If the IMSI is known in the RNC, the IMSI is provided to the core network in the connection-less interrogation message. The answer is based on the IMSI of the UE and the roaming agreements the CN operator has. If IMSI is not provided in the connection-less interrogation, the MSC/SGSN tries to retrieve the IMSI from the old MSC / old SGSN. The connection-less interrogation does not involve any UE or HLR communication. If the IMSI of the UE is not known in the core network, this is indicated in the interrogation response so that a connection-oriented procedure can be performed to retrieve the IMSI. If the IMSI is available in the core network(s) it is provided to the RNC in the interrogation response.

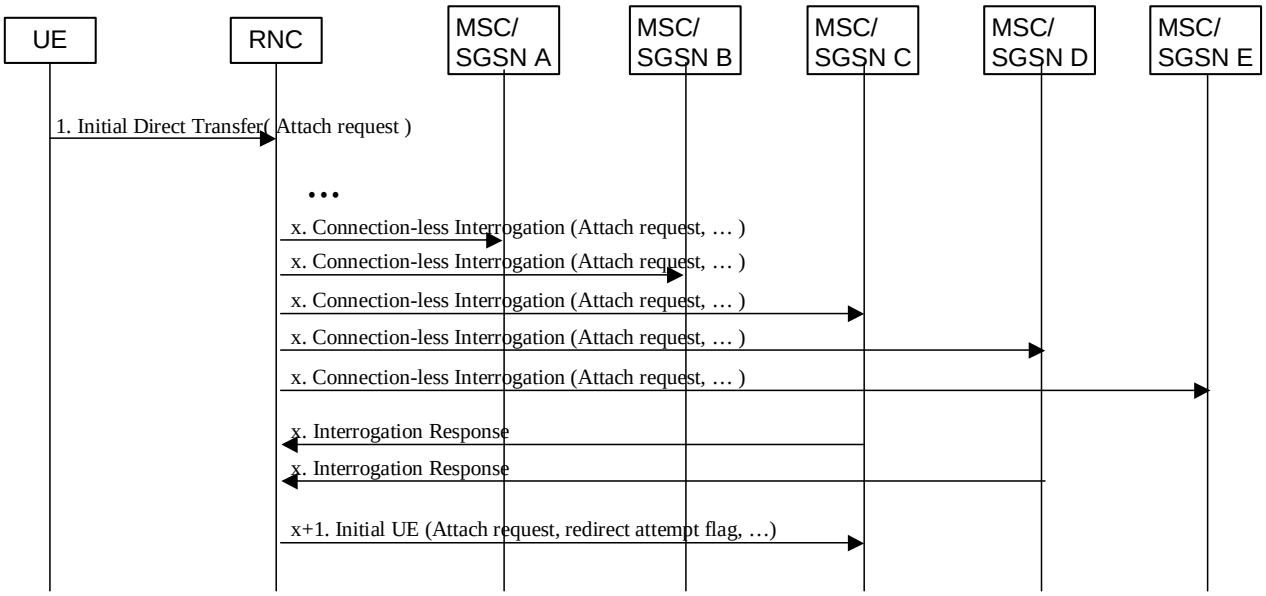

***Figure Z**, Connetion-less interrogation optimisation*