3GPP TSG SA WG3 Security — S3#31 **S3-030669**
18 - 21 November 2003
Munich, Germany

3GPP TSG CN WG4 Meeting #21 ***N4-031289***
Bangkok, Thailand, 27th – 31st October 2003

Title:	**LS on Special-RAND mechanism**
Response to:	S3-030653 (N4-031252) **LS on Special-RAND mechanism from SA3**
Release:	Rel-6
Source:	**CN4**
To:	**SA3**
Cc:	**CN1, GERAN2, T2**

Contact Person:

Name:	Ulrich Wiehe
Tel. Number:	+49 6621 169139
E-mail Address:	ulrich.wiehe@gksag.de

Attachments: **N4-031315 CR 29.002 (Rel-6) on addition of requestingPLMN-ID to Send Authentication Info Request**

1. Overall Description:

CN4 thank SA3 for their LS on Special RAND mechanism (S3-030653).
SA3's suggestion to extract the visited network identity from the lower layers of the MAP-stack i.e. from the SCCP calling party address of the request that arrives at the HLR/AuC and use it to determine uniquely the permitted algorithm settings was not over-enthusiastically well received by CN4. Although it may be possible as an implementation option to extract the needed information from the lower layer, CN4 do not endorse to mandate such behaviour.
As an alternative CN4 agreed to add the needed information (requesting PLMN-ID) as a parameter transferred on MAP level in the SendAuthenticationInfo request message. The CR introducing the new parameter in the MAP protocol is attached.

2. Actions:

none

3. Date of Next CN4 Meeting:

CN4 #22 16th February – 20th February 2004; Atlanta, USA

3GPP TSG CN WG4 Meeting #21
Bangkok, THAILAND, 27th – 31st October 2003

N4-031315

CR-Form-v7

CHANGE REQUEST

⌘	**29.002**	**CR**	**703**	⌘**rev**	**-**	⌘	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:	⌘	**Addition of requestingPLMN-ID to Send Authentication Info Request**			
Source:	⌘	Siemens			
Work item code:	⌘	TEI-6	***Date:***	⌘	28/10/2003
Category:	⌘	**B**	***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:	⌘	To meet SA3's requirement for the special RAND mechanism.
Summary of change:	⌘	Add the parameter requestingPLMN-ID to SendAuthenticationInfoArg.
Consequences if not approved:	⌘	Needed information must be extracted from the lower layer.

Clauses affected:	⌘	8.5.2, 17.7.1				
		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.

8.5.2 MAP_SEND_AUTHENTICATION_INFO service

8.5.2.1 Definition

This service is used between the VLR and the HLR for the VLR to retrieve authentication information from the HLR. The VLR requests up to five authentication vectors.

Also this service is used between the SGSN and the HLR for the SGSN to retrieve authentication information from the HLR. The SGSN requests up to five authentication vectors.

If the user is a UMTS subscriber, the HLR shall return authentication quintuplets. If the user is a GSM subscriber, the HLR shall return authentication triplets.

If the HLR cannot provide the VLR or the SGSN with triplets, an empty response is returned. The VLR or the SGSN may then re-use old authentication triplets, except where this is forbidden under the conditions specified in 3GPP TS 43.020 [24].

If the HLR cannot provide the VLR or the SGSN with quintuplets, an empty response is returned. The VLR or the SGSN shall not re-use old authentication quintuplets.

If the VLR or SGSN receives a MAP_SEND_AUTHENTICATION_INFO response containing a User Error parameter as part of the handling of an authentication procedure, the authentication procedure in the VLR or SGSN shall fail.

Security related network functions are further described in 3GPP TS 43.020 [24] and 3GPP TS 33.200.

The service is a confirmed service and consists of four service primitives.

8.5.2.2 Service primitives

The service primitives are shown in table 8.5/2.

Table 8.5/2: MAP_SEND_AUTHENTICATION_INFO parameters

Parameter name	Request	Indication	Response	Confirm
Invoke id	M	M(=)	M(=)	M(=)
IMSI	C	C(=)		
Number of requested vectors	C	C(=)		
Requesting node type	C	C(=)		
Re-synchronisation Info	C	C(=)		
Segmentation prohibited indicator	C	C (=)		
Immediate response preferred indicator	U	C (=)		
Requesting PLMN ID	C	C(=)		
AuthenticationSetList			C	C(=)
User error			C	C(=)
Provider error				O

8.5.2.3 Parameter use

Invoke id

See clause 7.6.1 for the use of this parameter.

IMSI

See clause 7.6.2 for the use of this parameter.

This parameter shall be present in the first (or only) request of the dialogue. If multiple service requests are present in a dialogue then this parameter shall not be present in any service request other than the first one.

Number of requested vectors

A number indicating how many authentication vectors the VLR or SGSN is prepared to receive. The HLR shall not return more vectors than indicated by this parameter.

This parameter shall be present in the first (or only) request of the dialogue. If multiple service requests are present in a dialogue then this parameter shall not be present in any service request other than the first one.

Requesting node type

The type of the requesting node (SGSN or VLR).

This parameter shall be present in the first (or only) request of the dialogue. If multiple service requests are present in a dialogue then this parameter shall not be present in any service request other than the first one.

Re-synchronisation Info

For definition and use of this parameter see 3GPP TS 33.200.

If multiple service requests are present in a dialogue then this parameter shall not be present in any service request other than the first one..

Segmentation prohibited indicator

This parameter indicates if the VLR or SGSN allows segmentation of the response at MAP user level.

This parameter may be present only in the first request of the dialogue.

Immediate response preferred indicator

This parameter indicates that one of the requested authentication vectors is requested for immediate use in the VLR or SGSN. It may be used by the HLR together with the number of requested vectors and the number of vectors stored in the HLR to determine the number of vectors to be obtained from the AuC. It shall be ignored if the number of available vectors is greater than the number of requested vectors.

If multiple service requests are present in a dialogue then this parameter shall not be present in any service request other than the first one.

Requesting PLMN ID

The PLMN-ID of the requesting node. See3GPP TS 23.003.

This parameter shall be present in the first (or only) request of the dialogue. If multiple service requests are present in a dialogue then this parameter shall not be present in any service request other than the first one.

AuthenticationSetList

A set of one to five authentication vectors are transferred from the HLR to the VLR or from the HLR to the SGSN, if the outcome of the service was successful.

User error

One of the following error causes defined in clause 7.6.1 shall be sent by the user in case of unsuccessful outcome of the service, depending on the respective failure reason:

- unknown subscriber;
- unexpected data value;
- system failure;
- data missing.

Provider error

See clause 7.6.1 for the use of this parameter.

.....

17.7.1 Mobile Service data types

.....

```
SendAuthenticationInfoArg ::= SEQUENCE {
    imsi                                 [0] IMSI,
    numberOfRequestedVectors             NumberOfRequestedVectors,
    segmentationProhibited               NULL                              OPTIONAL,
    immediateResponsePreferred           [1] NULL                           OPTIONAL,
    re-synchronisationInfo               Re-synchronisationInfo            OPTIONAL,
    extensionContainer                   [2] ExtensionContainer            OPTIONAL,
    ...,
    requestingNodeType                   [3] RequestingNodeType            OPTIONAL,
    requestingPLMN-Id                    [4] PLMN-Id                       OPTIONAL}
```

```
PLMN-Id ::= OCTET STRING (SIZE (3))
    -- The internal structure is defined as follows:
    -- octet 1 bits 4321                 Mobile Country Code 1st digit
    --         bits 8765                 Mobile Country Code 2nd digit
    -- octet 2 bits 4321                 Mobile Country Code 3rd digit
    --         bits 8765                 Mobile Network Code 3rd digit
    --                                   or filler (1111) for 2 digit MNCs
    -- octet 3 bits 4321                 Mobile Network Code 1st digit
    --         bits 8765                 Mobile Network Code 2nd digit
```