3GPP TSG CN Plenary **Tdoc NP-010086**
Meeting #11, Palm Springs, U.S.A
14th - 16th March 2001

Source:	**TSG CN WG4**
Title:	**CRs to Rel-4 on Work Item: Enhanced HE control of security**
Agenda item:	**8.14**
Document for:	**APPROVAL**

Introduction:

This document contains **1** CR on **Rel-4** Work Item **"SEC1-EHCS"**, that have been agreed by **TSG CN WG4**, and are forwarded to TSG CN Plenary meeting #11 for approval.

Spec	CR	Rev	Doc-2nd-Level	Phase	Subject	Cat	Ver_C
29.002	236	1	N4-010465	Rel-4	Requesting node type in authentication set request	B	4.2.1

CR-Form-v3

CHANGE REQUEST

⌘ **29.002** CR **236** ⌘ rev **1** ⌘ Current version: **4.2.1** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network X

Title: ⌘	Requesting node type in authentication set request	
Source: ⌘	CN4	
Work item code: ⌘	SEC1-EHCS	***Date:*** ⌘ 28 Feb 2001
Category: ⌘	**B**	***Release:*** ⌘ Rel-4

Use <u>one</u> of the following categories:
F (essential 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 <u>one</u> 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)

Reason for change: ⌘	To include the type of the requesting node in a request for authentication sets, as requested by SA3
Summary of change: ⌘	Add new information element, requesting node type, to the service and protocol definitions
Consequences if not approved: ⌘	

Clauses affected: ⌘	8.5.2; 17.7.1
Other specs affected: ⌘	☐ Other core specifications ⌘ CR 33.102-xxx ☐ 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/3G_Specs/CRs.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://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 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 GSM 03.20 [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 GSM 03.20 and 3G TS 33.102.

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 (=)		
AuthenticationSetList			C	C(=)
User error			C	C(=)
Provider error				O

8.5.2.3 Parameter use

Invoke id

See subclause 7.6.1 for the use of this parameter.

IMSI

See subclause 7.6.2 for the use of this parameter.

If segmentation is used this parameter shall not be present in subsequent segments.

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.

If segmentation is used this parameter shall not be present in subsequent segments.

<u>Requesting node type</u>

<u>The type of the requesting node (SGSN or VLR).</u>

<u>This parameter shall be present in the first (or only) request of the dialogue. If segmentation is used this parameter shall not be present in subsequent segments.</u>

<u>Re-synchronisation Info</u>

For definition and use of this parameter see 3G TS 33.102.

If segmentation is used this parameter shall not be present in subsequent segments.

<u>Segmentation prohibited indicator</u>

This parameter indicates if the VLR or SGSN allows message segmentation.

If segmentation is used this parameter shall not be present in subsequent segments.

<u>Immediate response preferred indicator</u>

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 segmentation is used this parameter shall not be present in subsequent segments.

<u>AuthenticationSetList</u>

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.

<u>User error</u>

One of the following error causes defined in subclause 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.

<u>Provider error</u>

See subclause 7.6.1 for the use of this parameter.

**** Next modified section ****

17.7.1 Mobile Service data types

```
MAP-MS-DataTypes {
   ccitt identified-organization (4) etsi (0) mobileDomain (0)
   gsm-Network (1) modules (3) map-MS-DataTypes (11) version7 (7)}

DEFINITIONS
...
-- authentication management types
```

```
SendAuthenticationInfoArg ::= SEQUENCE {
    imsi                              [0] IMSI,
    numberOfRequestedVectors          NumberOfRequestedVectors,
    segmentationProhibited            NULL                        OPTIONAL,
    -- if segmentation is prohibited the HLR shall not send the result within
    -- a TC-CONTINUE message.
    immediateResponsePreferred        [1] NULL                    OPTIONAL,
    -- if present, the HLR may send an immediate response with the available authentication
    -- vectors (see § 8.5.2 for more information).
    re-synchronisationInfo            Re-synchronisationInfo      OPTIONAL,
    extensionContainer                [2] ExtensionContainer      OPTIONAL,
    ...,
    requestingNodeType                [3] RequestingNodeType      OPTIONAL}
```

```
NumberOfRequestedVectors ::= INTEGER (1..5)
```

```
Re-synchronisationInfo ::= SEQUENCE {
    rand                              RAND,
    auts                              AUTS,
    ...}
```

```
SendAuthenticationInfoRes ::= [3] SEQUENCE {
    authenticationSetList             AuthenticationSetList       OPTIONAL,
    extensionContainer                ExtensionContainer          OPTIONAL,
    ...}
```

```
RequestingNodeType ::= ENUMERATED {
    vlr   (0),
    sgsn  (1),
    ...}
    -- exception handling:
    -- received values in the range 2-15 shall be treated as "vlr"
    -- received values greater than 15 shall be treated as "sgsn"
```