3GPP TSG_CN **Tdoc NP-000326**
Plenary Meeting #8, Dusseldorf, Germany
21st – 23rd June 2000.

Source: **TSG_N WG4**

Title: **CRs to 3G Work Item "Security" for Release 99**

Agenda item: **6.3.4**

Document for: **APPROVAL**

Introduction:

This document contains **"2"** CRs on **Work Item "Security" for Release 99,** that have been agreed by **TSG_N WG4,** and are forwarded to **TSG_N Plenary** meeting #8 for approval.

TDoc	SPEC	CR	REV	PHAS	VERS	SUBJECT	CAT	NEW_VERS
N4-000399	24.010	001		R99	3.0.0	Alignment of SS protocol with current MM/GMM integrity	C	3.1.0
N4-000264	29.002	138		R99	3.4.0	Clarification of SAI-ack segmentation procedure	F	3.5.0

Tdoc N4-000399

3GPP-CN1/SMG3WPA Meeting #12
Oahu/Hawaii, USA. 22-26 May, 2000

Document *N1-000746*
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

24.010 **CR** **001** Current Version: 3.0.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to: CN #08 for approval ☒ strategic □ *(for SMG*
list expected approval meeting # here ↑ for information □ non-strategic ☒ *use only)*

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: (U)SIM □ ME ☒ UTRAN / Radio □ Core Network ☒
(at least one should be marked with an X)

Source: N4 **Date:** 17th May 2000

Subject: Alignment of SS protocol with current MM/GMM integrity protection rules

Work item: Security

Category:	F	Correction	□	**Release:**	Phase 2	□
	A	Corresponds to a correction in an earlier release	□		Release 96	□
(only one category	B	Addition of feature	□		Release 97	□
shall be marked	C	Functional modification of feature	☒		Release 98	□
with an X)	D	Editorial modification	□		Release 99	☒
					Release 00	□

Reason for change: In UMTS, all signalling messages for all protocols shall be integrity protected. This CR adds that requirement to the SS protocol description.

Clauses affected: 2.2.1

Other specs	Other 3G core specifications	☒	→ List of CRs:	24.008 – N1-000745 24.011 - N1-000747
affected:	Other GSM core specifications	□	→ List of CRs:	
	MS test specifications	□	→ List of CRs:	
	BSS test specifications	□	→ List of CRs:	
	O&M specifications	□	→ List of CRs:	

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

2.2 Functional procedures for the control of supplementary services

2.2.1 General

This clause specifies the functional signalling procedures for the control of supplementary services at the radio interface.

The Functional protocol utilizes functions and services provided by GSM 04.08 basic call control procedures and the functions of the data link layer as defined in GSM 04.06.

In UMTS only, integrity protected signalling (see ~~section 4.1.1.1.1 of~~ TS 24.008, subclause ‘Integrity Protection of Signalling Messages,’ and in general, see TS 33.102) is mandatory. In UMTS only, all protocols shall use integrity protected signalling. Integrity protection of all ~~layer 3~~SS signalling messages is the responsibility of lower layers. It is the network which activates integrity protection. This is done using the security mode control procedure (TS 25.331).

The defined procedures specify the basic methodology for the control (e.g. registration, erasure, invocation, etc.) of supplementary services.

The first category, called the Separate Message Category utilizes separate message types to indicate a desired function. The hold and retrieve families of messages are identified for this category.

The second category called the Common Information Element Category utilizes the Facility information element to transport the protocol defined in GSM 04.80. The use of the Facility information element is common to many services, and its contents indicates what type of procedure is being requested. This category can be signalled both in the mobile to network and the network to mobile directions.

The control of supplementary services includes the following cases:

a) the request of supplementary service procedures during the establishment of a call;

b) the request of supplementary service procedures during the clearing of a call;

c) the request of call related supplementary service procedures during the active state of a call;

d) the request of supplementary service procedures independent from an active call;

e) the request of multiple, different supplementary service procedures within a single message;

f) the request of supplementary service procedures related to different calls.

The correlation of a call related supplementary service operation and the call which it modifies is provided by use of the transaction identifier (cases a, b, c, e and f).

The correlation of supplementary service operations and their responses, is provided by the combination of the transaction identifier of the messages containing the Facility information element and the Invoke identifier present within the Facility information element itself (cases a, b, c, d, e and f).

The identification of different supplementary service operations within one single message is provided by the Invoke identifier present within the Facility information element itself (case e).

The identification of supplementary service related operations to different calls is provided by using different messages with the corresponding transaction identifier of the appropriate call (case f), i.e. different transaction identifier values are used to identify each call individually.

3GPP TSG-CN WG4

Rotenburg a.d. Fulda, Hessen, Germany, 22-26 May 2000

Document N4-000264

e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

29.002	**CR**	**138**	Current Version:	3.4.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ ↑ *CR number as allocated by MCC support team*

For submission to:	CN#8	for approval	**X**	strategic		*(for SMG*
list expected approval meeting # here ↑		for information		non-strategic	X	*use only)*

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects:	(U)SIM	□	ME	□	UTRAN / Radio	□	Core Network	**X**

(at least one should be marked with an X)

Source:	N4	**Date:**	15 May 2000
Subject:	Clarification of SAI-ack segmentation procedure		
Work item:	UMTS Security		

Category:	F	Correction	**X**	**Release:**	Phase 2	□
	A	Corresponds to a correction in an earlier release	□		Release 96	□
(only one category	B	Addition of feature	□		Release 97	□
shall be marked	C	Functional modification of feature	□		Release 98	□
with an X)	D	Editorial modification	□		Release 99	**X**
					Release 00	□

Reason for change:	Clarification of use of the MAP_SEND_AUTHENTICATION_INFO service to request additional authentication vectors from the HLR using segmentation.
Clauses affected:	8.5.2, 17.6.1, 17.7.1, 25.5.4

Other specs affected:	Other 3G core specifications	□	→ List of CRs:
	Other GSM core specifications	□	→ List of CRs:
	MS test specifications	□	→ List of CRs:
	BSS test specifications	□	→ List of CRs:
	O&M specifications	□	→ List of CRs:

Other comments:	This CR ensures that no parameters should be sent is subsequent MAP_SEND_AUTHENTICATION_INFO requests, simplifying parameter processing and error procedures in the HLR for subsequent MAP_SEND_AUTHENTICATION_INFO requests.

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	~~M~~C	C~~M~~(=)		
Number of requested vectors	~~M~~C	C~~M~~(=)		
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.

Re-synchronisation Info

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.

Segmentation prohibited indicator

This parameter indicates if the VLR or SGSN allows message segmentation.
If segmentation is used this parameter shall not be present in subsequent segments.

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

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 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.

Provider error

See subclause 7.6.1 for the use of this parameter.

17.6 MAP operation and error types

17.6.1 Mobile Service Operations

```
MAP-MobileServiceOperations {
   ccitt identified-organization (4) etsi (0) mobileDomain (0)
   gsm-Network (1) modules (3) map-MobileServiceOperations (5)
   version6 (6)}

...
```

```
PrepareSubsequentHandover ::= OPERATION                                    --Timer m
     ARGUMENT
          prepareSubsequentHO-Arg         PrepareSubsequentHO-Arg
     RESULT
          prepareSubsequentHO-Res         PrepareSubsequentHO-Res
     ERRORS {
          UnexpectedDataValue,
          DataMissing,
          UnknownMSC,
          SubsequentHandoverFailure}
```

```
-- authentication management operations
```

```
SendAuthenticationInfo ::= OPERATION                                       --Timer m
     ARGUMENT
          sendAuthenticationInfoArg       SendAuthenticationInfoArg
          -- optional
          -- if segmentation is used, sendAuthenticationInfoArg shall be present in the first
          -- segment and shall not be present in subsequent segments.  If received in
          -- subsequent segments it shall be discarded.

     RESULT
          sendAuthenticationInfoRes       SendAuthenticationInfoRes
          -- optional
     ERRORS {
          SystemFailure,
          DataMissing,
          UnexpectedDataValue,
          UnknownSubscriber}
```

17.7 MAP constants and data types

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) version6 (6)}

...
```

```
maxNumOfEncryptionInfo INTEGER ::= 100
```

```
-- authentication management types
```

```
SendAuthenticationInfoArg ::= SEQUENCE {
     imsi                                [0] IMSI,
     numberOfRequestedVectors            NumberOfRequestedVectors~~          OPTIONAL~~,
~~     -- if segmentation is used, numberOfRequestedVectors shall be present in~~
~~     -- the first segment and shall not be present in subsequent segments. If received~~
~~     -- in a subsequent segment it shall be discarded.~~
     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).
~~     -- if segmentation is used, immediateResponsePreferred shall not be present in~~
~~     -- subsequent segments. If received in a subsequent segment it shall be discarded.~~
     re-synchronisationInfo              Re-synchronisationInfo              OPTIONAL,
     extensionContainer                  [2] ExtensionContainer              OPTIONAL,
     ...}
```

25.5.4 Macro Obtain_Authent_Para_VLR

This macro is used by the VLR to request authentication vectors from the HLR. The macro proceeds as follows:

- a connection is opened, and a MAP_SEND_AUTHENTICATION_INFO request sent to the HLR;
- if the HLR indicates that a MAP version 1 or 2 dialogue is to be used, the VLR performs the equivalent MAP version 1 or 2 dialogue. which can return a positive result containing authentication sets, an empty positive result, or an error;
- if the dialogue opening fails, the "Procedure Error" exit is used. Otherwise, the VLR waits for the response from the HLR;
- if a MAP_SEND_AUTHENTICATION_INFO confirmation is received from the HLR, the VLR checks the received data.

One of the following positive responses may be received from a MAP version 1 or MAP version 2 dialogue with the HLR:

- Authentication triplets, in which case the outcome is successful;
- Empty response, in which case the VLR may re-use old triplets, if allowed by the PLMN operator.

If the VLR cannot re-use old triplets (or no such triplets are available) then the "Procedure Error" exit is used.

If the outcome was successful or re-use of old parameters in the VLR is allowed, then the "OK" exit is used.

If an "Unknown Subscriber" error is returned by the MAP version 1 or 2 dialogue, then the "Unknown Subscriber" exit is used.

In a MAP version 3 dialogue a (possibly empty) set of authentication vectors may be received from the HLR followed by a MAP_CLOSE_Indication or by a MAP_DELIMITER_Indication. If a MAP_DELIMITER_Indication is received, the VLR may request additional authentication vectors from the HLR by sending a new MAP_SEND_AUTHENTIFICATION_INFO_Request with no parameter part. If a MAP_CLOSE_Indication is received, and authentication vectors have been received during the dialogue, then the "OK" exit is used. If no authentication vectors have been received during the dialogue, the VLR checks whether old GSM Triplets are available and can be re-used. If so, the "OK" exit is used, otherwise the "Procedure Error" exit is used. Note that re-use of old UMTS Quintuplets is not allowed.

If in a MAP version 3 dialogue an "Unknown Subscriber" error is received, then the "Unknown Subscriber" exit is used. If other errors are received, the VLR checks whether old GSM Triplets are available and can be re-used. If so, the "OK" exit is used, otherwise the "Procedure Error" exit is used. Note that re-use of old UMTS Quintuplets is not allowed.

- if a MAP-U-ABORT, MAP_P_ABORT, MAP_NOTICE or unexpected MAP_CLOSE service indication is received from the MSC, then open connections are terminated, and the macro takes the "Null" exit;
- if a MAP-U-ABORT, MAP_P_ABORT or unexpected MAP_CLOSE service indication is received from the HLR, then the VLR checks whether old authentication parameters (GSM triplets) can be re-used. If old parameters cannot be re-used the macro takes the "Procedure Error" exit; otherwise it takes the "OK" exit; note that re-use of old UMTS Quintuplets is not allowed;
- if a MAP_NOTICE service indication is received from the HLR, then the dialogue with the HLR is closed. The VLR then checks whether old authentication parameters (GSM triplets) can be re-used. If old parameters cannot be re-used the macro takes the "Procedure Error" exit; otherwise it takes the "OK" exit; note that re-use of old UMTS Quintuplets is not allowed.

The macro is described in figure 25.5/4.