3GPP TSG SA WG3 Security — S3#15 **S3-000503**

12-14 September, 2000

Washington D.C., USA

3GPP TSG CN Working Group 4 **N4-000537**
CN4#03 Meeting,
Helsinki, Finland
17 - 21 July 2000

Source: **TSG CN WG4**[1]

To: **CN WG1**

CC: **SA WG3**

Title: **Liaison statement on the modified lengths of parameters AUTN and AUTS**

CN4 noticed, serendipitously, that TSG SA approved CR 33.103-009, which modifies the AUTN and AUTS parameter lengths from variable to fixed. This change has an impact on TS 29.002, which has been properly addressed in CR 29.002-151.

CN1 are kindly asked to review the above mentioned CR against TS 33.103, to see if there is a similar impact on TS 24.008

[1] Contact: Luis López-Soria, Ericsson L.M.; tel. +34 91 339 2656; email: luis.lopez-soria@ece.ericsson.se

3GPP TSG CN WG4 #3
Helsinki, Finland, 17-21 Jul 2000

Document N4-000428
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**	**151**	Current Version:	3.5.0

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

For submission to:	CN#09	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic	X	

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: Ericsson L.M. **Date:** 2000-06-29

Subject: AUTS and AUTN parameter length

Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction	X	**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: In TS 33.105 v3.3.0, section 5.1.7.3, the length of SQN is fixed to 48 bits.
The length of parameters AUTS and AUTN was modified accordingly (from variable to fixed) in CR 33.103-009, which was approved in the SA3 #13 meeting in Yokohama.

Clauses affected: 17.7.1

Other specs affected:

Other 3G core specifications	X	→ 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:


help.doc

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

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)}

DEFINITIONS

IMPLICIT TAGS

::=

BEGIN

EXPORTS

      -- location registration types
      UpdateLocationArg,
      UpdateLocationRes,
      CancelLocationArg,
      CancelLocationRes,
      PurgeMS-Arg,
      PurgeMS-Res,
      SendIdentificationArg,
      SendIdentificationRes,
      UpdateGprsLocationArg,
      UpdateGprsLocationRes,
      IST-SupportIndicator,


      -- handover types
      ForwardAccessSignalling-Arg,
      PrepareHO-Arg,
      PrepareHO-Res,
      PrepareSubsequentHO-Arg,
      PrepareSubsequentHO-Res,
      ProcessAccessSignalling-Arg,
      SendEndSignal-Arg,
      SendEndSignal-Res,


      -- authentication management types
      SendAuthenticationInfoArg,
      SendAuthenticationInfoRes,
      AuthenticationFailureReportArg,
   AuthenticationFailureReportRes,

      -- security management types
      EquipmentStatus,
      Kc,

      -- subscriber management types
      InsertSubscriberDataArg,
      InsertSubscriberDataRes,
      DeleteSubscriberDataArg,
      DeleteSubscriberDataRes,
      SubscriberData,
      ODB-Data,
      SubscriberStatus,
      ZoneCodeList,
      maxNumOfZoneCodes,
      O-CSI,
   D-CSI,
      O-BcsmCamelTDPCriteriaList,
      T-BCSM-CAMEL-TDP-CriteriaList,
      SS-CSI,
      ServiceKey,
      DefaultCallHandling,
      CamelCapabilityHandling,
      BasicServiceCriteria,
      SupportedCamelPhases,
      maxNumOfCamelTDPData,
      CUG-Index,
      CUG-Interlock,
      InterCUG-Restrictions,
      IntraCUG-Options,
      NotificationToMSUser,
   IST-AlertTimerValue,
      T-CSI,
      T-BcsmTriggerDetectionPoint,
```

```
      -- fault recovery types
      ResetArg,
      RestoreDataArg,
      RestoreDataRes,

      -- subscriber information enquiry types
      ProvideSubscriberInfoArg,
      ProvideSubscriberInfoRes,
      SubscriberInfo,
      LocationInformation,
      SubscriberState,

      -- any time information enquiry types
      AnyTimeInterrogationArg,
      AnyTimeInterrogationRes,

      -- any time information handling types
      AnyTimeSubscriptionInterrogationArg,
      AnyTimeSubscriptionInterrogationRes,
      AnyTimeModificationArg,
      AnyTimeModificationRes,

      -- subscriber data modification notification types
      NoteSubscriberDataModifiedArg,
      NoteSubscriberDataModifiedRes,

      -- gprs location information retrieval types
      SendRoutingInfoForGprsArg,
      SendRoutingInfoForGprsRes,

      -- failure reporting types
      FailureReportArg,
      FailureReportRes,

      -- gprs notification types
      NoteMsPresentForGprsArg,
      NoteMsPresentForGprsRes,

      -- Mobility Management types
   NoteMM-EventArg,
      NoteMM-EventRes



;

IMPORTS
      maxNumOfSS,
      SS-SubscriptionOption,
      SS-List,
      SS-ForBS-Code,
      Password
FROM MAP-SS-DataTypes {
   ccitt identified-organization (4) etsi (0) mobileDomain (0)
   gsm-Network (1) modules (3) map-SS-DataTypes (14) version6 (6)}

      SS-Code
FROM MAP-SS-Code {
   ccitt identified-organization (4) etsi (0) mobileDomain (0)
   gsm-Network (1) modules (3) map-SS-Code (15) version6 (6)}

      Ext-BearerServiceCode
FROM MAP-BS-Code {
   ccitt identified-organization (4) etsi (0) mobileDomain (0)
   gsm-Network (1) modules (3) map-BS-Code (20) version6 (6)}

      Ext-TeleserviceCode
FROM MAP-TS-Code {
   ccitt identified-organization (4) etsi (0) mobileDomain (0)
   gsm-Network (1) modules (3) map-TS-Code (19) version6 (6)}


      AddressString,
   ISDN-AddressString,
      ISDN-SubaddressString,
      FTN-AddressString,
      AccessNetworkSignalInfo,
      IMSI,
      TMSI,
      HLR-List,
      LMSI,
```

```
      Identity,
      GlobalCellId,
      CellGlobalIdOrServiceAreaIdOrLAI,
      Ext-BasicServiceCode,
      NAEA-PreferredCI,
      EMLPP-Info,
      MC-SS-Info,
      SubscriberIdentity,
      AgeOfLocationInformation,
      LCSClientExternalID,
      LCSClientInternalID,
      Ext-SS-Status


FROM MAP-CommonDataTypes {
   ccitt identified-organization (4) etsi (0) mobileDomain (0)
   gsm-Network (1) modules (3) map-CommonDataTypes (18) version6 (6)}

      ExtensionContainer
FROM MAP-ExtensionDataTypes {
   ccitt identified-organization (4) etsi (0) mobileDomain (0)
   gsm-Network (1) modules (3) map-ExtensionDataTypes (21) version6 (6)}

      AbsentSubscriberDiagnosticSM
FROM MAP-ER-DataTypes {
   ccitt identified-organization (4) etsi (0) mobileDomain (0)
   gsm-Network (1) modules (3) map-ER-DataTypes (17) version6 (6)}


;


-- location registration types

UpdateLocationArg ::= SEQUENCE {
     imsi                                IMSI,

     msc-Number                          [1] ISDN-AddressString,
     vlr-Number                          ISDN-AddressString,
     lmsi                                [10] LMSI OPTIONAL,
     extensionContainer                  ExtensionContainer                OPTIONAL,
     ... ,
     vlr-Capability                      [6] VLR-Capability                OPTIONAL }

VLR-Capability ::= SEQUENCE{
     supportedCamelPhases                [0] SupportedCamelPhases          OPTIONAL,
     extensionContainer                  ExtensionContainer                OPTIONAL,
     ... ,
     solsaSupportIndicator               [2] NULL                          OPTIONAL,
     istSupportIndicator                 [1] IST-SupportIndicator          OPTIONAL,
     superChargerSupportedInServingNetworkEntity   [3] SuperChargerInfo    OPTIONAL,
     longFTN-Supported                   [4]  NULL                         OPTIONAL }

SuperChargerInfo ::= CHOICE {
     sendSubscriberData                  [0] NULL,
     subscriberDataStored                [1] AgeIndicator }

AgeIndicator ::= OCTET STRING (SIZE (1..6))
     -- The internal structure of this parameter is implementation specific.

IST-SupportIndicator ::=  ENUMERATED {
     basicISTSupported                   (0),
     istCommandSupported                 (1),
     ...}
-- exception handling:
-- reception of values > 1 shall be mapped to ' istCommandSupported '

UpdateLocationRes ::= SEQUENCE {
     hlr-Number                          ISDN-AddressString,

     extensionContainer                  ExtensionContainer                OPTIONAL,
     ... }
```

```
CancelLocationArg ::= [3] SEQUENCE {
     identity                              Identity,
     cancellationType                      CancellationType                 OPTIONAL,
     extensionContainer                    ExtensionContainer               OPTIONAL,
     ...}
```

```
CancellationType ::= ENUMERATED {
     updateProcedure                       (0),
     subscriptionWithdraw                  (1),
     ...}
     -- The HLR shall not send values other than listed above
```

```
CancelLocationRes ::= SEQUENCE {
     extensionContainer                    ExtensionContainer               OPTIONAL,
     ...}
```

```
PurgeMS-Arg ::= [3] SEQUENCE {
     imsi                                  IMSI,
     vlr-Number                            [0] ISDN-AddressString           OPTIONAL,
     sgsn-Number                           [1]  ISDN-AddressString          OPTIONAL,
     extensionContainer                    ExtensionContainer               OPTIONAL,
     ...}
```

```
PurgeMS-Res ::= SEQUENCE {
     freezeTMSI                            [0]  NULL                        OPTIONAL,
     freezeP-TMSI                          [1]  NULL                        OPTIONAL,
     extensionContainer                    ExtensionContainer               OPTIONAL,
     ...}
```

```
SendIdentificationArg ::= SEQUENCE {
     tmsi                                  TMSI,
     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 previous VLR shall not send the result
     -- within a TC-CONTINUE message.
     extensionContainer                    ExtensionContainer               OPTIONAL,
     ...}
```

```
SendIdentificationRes ::= [3] SEQUENCE {
     imsi                                  IMSI                             OPTIONAL,
     -- IMSI must be present if SendIdentificationRes is not segmented.
     -- If the TC-Continue segmentation option is taken the IMSI must be
     -- present in one segmented transmission of SendIdentificationRes.
     authenticationSetList                 AuthenticationSetList            OPTIONAL,
     currentSecurityContext                [2]CurrentSecurityContext        OPTIONAL,
     extensionContainer                    [3] ExtensionContainer           OPTIONAL,
     ...}
```

```
-- authentication management types
```

```
AuthenticationSetList ::= CHOICE {
     tripletList                           [0] TripletList,
     quintupletList                        [1] QuintupletList }
```

```
TripletList ::= SEQUENCE SIZE (1..5) OF
                                           AuthenticationTriplet
```

```
QuintupletList ::= SEQUENCE SIZE (1..5) OF
                                           AuthenticationQuintuplet
```

```
AuthenticationTriplet ::= SEQUENCE {
     rand                                  RAND,
     sres                                  SRES,
     kc                                    Kc,
     ...}
```

```
AuthenticationQuintuplet ::= SEQUENCE {
     rand                                  RAND,
     xres                                  XRES,
     ck                                    CK,
     ik                                    IK,
     autn                                  AUTN,
     ...}
```

```
CurrentSecurityContext ::= CHOICE {
     gsm-SecurityContextData              [0] GSM-SecurityContextData,
     umts-SecurityContextData             [1] UMTS-SecurityContextData }
```

```
GSM-SecurityContextData ::= SEQUENCE {
     kc                                   Kc,
     cksn                                 Cksn,
     ... }
```

```
UMTS-SecurityContextData ::= SEQUENCE {
     ck                                   CK,
     ik                                   IK,
     ksi                                  KSI,
     ... }
```

```
RAND ::= OCTET STRING (SIZE (16))
```

```
SRES ::= OCTET STRING (SIZE (4))
```

```
Kc ::= OCTET STRING (SIZE (8))
```

```
XRES ::= OCTET STRING (SIZE (4..16))
```

```
CK ::= OCTET STRING (SIZE (16))
```

```
IK ::= OCTET STRING (SIZE (16))
```

```
AUTN ::= OCTET STRING (SIZE (164..18))
```

```
AUTS ::= OCTET STRING (SIZE (142..16))
```