**3GPP TSG WG SA3#17** ***Tdoc S3-010006***
**Gothenberg, Sweden, 27 Februar- 3 March 2001**

*CR-Form-v3*

# CHANGE REQUEST

⌘ **33.102** **CR** **CR-Num** ⌘ rev **-** ⌘ Current version: **3.7.0** ⌘

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

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

| | | |
|---|---|---|
| ***Title:*** | ⌘ | RES has to be a multiple of 8 bits |
| ***Source:*** | ⌘ | Siemens Atea |
| ***Work item code:*** | ⌘ | Security ***Date:*** ⌘ 19/2/2001 |
| ***Category:*** | ⌘ | **F** ***Release:*** ⌘ R99 |

*Use one 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 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)*

***Reason for change:*** ⌘ -Other specifications have no protocol-provisions to handle bits for XRES

A) TS 29.002 (MAP) specify XRES as OCTET STRING.
"XRES **::= OCTET STRING (SIZE (4..16))"**

B) TS 24.008 (Mobile Radio layer 3 Specification) specify RES as number of octets.
**"**The Authentication Response parameter (extension) IE is a type 4 information element with a minimum length of 3 octets and a maximum length of 14 octets"

- All other Authentication Parameters are specified as bits, but match a multiple of 8 bits.

***Summary of change:*** ⌘ RES definition is aligned to a multiple of 8 bits (octet) too.

***Consequences if not approved:*** ⌘ TS 29.002 and TS 24.008 have to be adapted to handle bit-variable RES.

***Clauses affected:*** ⌘ 6.3.7
6.8.1.2

***Other specs affected:*** ⌘
☐ 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/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.

## 6.3.7 Length of authentication parameters

The authentication key (K) shall have a length of 128 bits.

The random challenge (RAND) shall have a length of 128 bits.

Sequence numbers (SQN) shall have a length of 48 bits.

The anonymity key (AK) shall have a length of 48 bits.

The authentication management field (AMF) shall have a length of 16 bits.

The message authentication codes MAC in AUTN and MAC-S in AUTS shall have a length of 64 bits.

The cipher key (CK) shall have a length of 128 bits.

The integrity key (IK) shall have a length of 128 bits.

The authentication response (RES) shall have a variable length of 4-16 octets~~32-128 bits~~.

### 6.8.1.2 R99+ HLR/AuC

Upon receipt of an *authentication data request* from a R99+ VLR/SGSN for a UMTS subscriber, a R99+ HLR/AuC shall send quintets, generated as specified in 6.3.

Upon receipt of an *authentication data request* from a R98- VLR/SGSN for a UMTS subscriber, a R99+ HLR/AuC shall send triplets, derived from quintets using the following conversion functions:

a) c1: $RAND_{[GSM]} = RAND$

b) c2: $SRES_{[GSM]} = XRES^*_1$ xor $XRES^*_2$ xor $XRES^*_3$ xor $XRES^*_4$

c) c3: $Kc_{[GSM]} = CK_1$ xor $CK_2$ xor $IK_1$ xor $IK_2$

whereby XRES* is 16 octet~~128 bits~~ long and XRES* = XRES if XRES is 16 octet~~128 bits~~ long and XRES* = XRES || 0...0 if XRES is shorter than 16 octet~~128 bits~~, $XRES^*_i$ are all 4 octet~~32 bit~~ long and $XRES^* = XRES^*_1 \| XRES^*_2 \| XRES^*_3 \| XRES^*_4$, $CK_i$ and $IK_i$ are both 64 bits long and $CK = CK_1 \| CK_2$ and $IK = IK_1 \| IK_2$.