*CR-Form-v3*

# CHANGE REQUEST

⌘ **33.105**     CR **CR-Num** ⌘ rev **-** ⌘ Current version: **3.6.0** ⌘

*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 **x**

| | | |
|---|---|---|
| ***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<br><br>A) TS 29.002 (MAP) specify XRES as OCTET STRING.<br> "XRES **::= OCTET STRING (SIZE (4..16))**"<br><br>B) TS 24.008 (Mobile Radio layer 3 Specification) specify RES as number of octets.<br> "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"<br><br>- All other Authentication Parameters are specified as bits, but match a multiple of 8 bits. |
| ***Summary of change:*** ⌘ | RES definition is aligned to 8bits (Octet). |
| ***Consequences if not approved:*** ⌘ | TS 29.002 and TS 24.008 have to be adapted to handle bit-variable RES. |

| | |
|---|---|
| ***Clauses affected:*** ⌘ | 5.1.7.8 |

| | | |
|---|---|---|
| ***Other specs affected:*** ⌘ | ☐ Other core specifications ⌘<br>☐ Test specifications<br>☐ 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.

## 5.1.7.8    RES (or XRES)

RES: the user response

RES[0], RES[1], …, RES[n-1]

The length n of RES and XRES is at most 128 bits and at least 32 bits, and shall be a multiple of 8 bits. RES and XRES constitute to entity authentication of the user to the network.