

CHANGE REQUEST

⌘ **33.203** CR **CRNum** ⌘ rev **-** ⌘ Current version: **5.2.0** ⌘

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: | ⌘ The definition of the key to be used for HMAC-SHA1-96 within ESP | | |
| Source: | ⌘ SA WG3 | | |
| Work item code: | ⌘ IMS-ASEC | Date: | ⌘ July 10 2002 |
| Category: | ⌘ F Use <u>one</u> of the following categories: F (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 . | Release: | ⌘ Rel-5 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: | ⌘ Create conformity with IETF RFC 2104 |
| Summary of change: | ⌘ Specifies how to expand IK from 128 bits to 160 bits |
| Consequences if not approved: | ⌘ TS 33.203 will not follow the principles as specified in IETF RFC 2104 |

| | |
|------------------------------|--|
| Clauses affected: | ⌘ Annex I |
| Other specs affected: | ⌘ <input type="checkbox"/> Other core specifications ⌘ <input type="checkbox"/> Test specifications <input type="checkbox"/> O&M Specifications |
| Other comments: | ⌘ |

***** FIRST CHANGED SECTION *****

Annex I (normative): Key expansion functions for IPsec ESP

If the selected authentication algorithm is HMAC-MD5-96 then $IK_{ESP} = IK_{IM}$.

If the selected authentication algorithm is HMAC-SHA-1-96 then IK_{ESP} is obtained from IK_{IM} by appending ~~the 32 most significant bits~~32 zero bits of IK_{IM} to the end of IK_{IM} to create a 160-bit string.
