Technical Specification Group Services and System Aspects
Meeting #24, Seoul, South Korea, 07 - 10 June 2004

**TSGS#24(04)0377**

**Source:** **SA WG3 (Security)**

**Title:** **CR to 33.220: Removal of editors notes on Transaction Identifiers (Rel-6)**

**Document for:** **Approval**

**Agenda Item:** **7.3.3**

| SA Doc number | Spec | CR | Rev | Phase | Subject | Cat | Version-Current | SA WG3 Doc number | Workitem |
|---|---|---|---|---|---|---|---|---|---|
| SP-040377 | 33.220 | 003 | - | Rel-6 | Removal of editors notes on Transaction Identifiers | D | 6.0.0 | S3-040410 | SEC1-SC |

**3GPP TSG-SA WG3 Meeting #33**
**10th – 14th May 2004, Beijing, China**

***Tdoc* ⌘*S3-040410***

CR-Form-v7

# CHANGE REQUEST

|  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|
| ⌘ | **33.220** | **CR** | **003** | ⌘**rev** | **-** | ⌘ | Current version: | **6.0.0** | ⌘ |

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

***Proposed change affects:*** UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

|  |  |  |  |  |  |
|---|---|---|---|---|---|
| ***Title:*** | ⌘ | Removal of editors notes on Transaction Identifiers | | | |
| ***Source:*** | ⌘ | SA WG3 | | | |
| ***Work item code:*** | ⌘ | SEC1-SC | ***Date:*** | ⌘ | 10/05/2004 |
| ***Category:*** | ⌘ | **D** | ***Release:*** | ⌘ | Rel-6 |
|  |  | *Use one of the following categories:*<br>***F*** *(correction)*<br>***A*** *(corresponds to a correction in an earlier release)*<br>***B*** *(addition of feature),*<br>***C*** *(functional modification of feature)*<br>***D*** *(editorial modification)*<br>Detailed explanations of the above categories can be found in 3GPP TR 21.900. | *Use one of the following releases:*<br>*2 (GSM Phase 2)*<br>*R96 (Release 1996)*<br>*R97 (Release 1997)*<br>*R98 (Release 1998)*<br>*R99 (Release 1999)*<br>*Rel-4 (Release 4)*<br>*Rel-5 (Release 5)*<br>*Rel-6 (Release 6)* | | |

|  |  |  |
|---|---|---|
| ***Reason for change:*** | ⌘ | Both removed editors notes are no longer necessary |
| ***Summary of change:*** | ⌘ | First Note: Content generally out of scope of this specification. Replaced by Note stating this and giving HTTP Digest example.<br>Second Note: Not appliccable under this heading, therefore deleted. (General problem also solved by key lifetime and key renegotiation) |
| ***Consequences if not approved:*** | ⌘ | First Note: Wrong statement.<br>Second Note: superfluous Note. |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 4.3.7 | | | | |
|  |  | **Y** | **N** |  |  |  |
| ***Other specs affected:*** | ⌘ |  | **X** | Other core specifications | ⌘ | none |
|  |  |  | **X** | Test specifications |  |  |
|  |  |  | **X** | O&M Specifications |  |  |
| ***Other comments:*** | ⌘ |  |  |  |  |  |

**************************** begin change ******************************

### 4.3.7 Requirements on Transaction Identifier

Transaction identifier shall be used to bind the subscriber identity to the keying material in Ua, Ub and Zn interfaces.

Requirements for Transaction Identifier are:

- Transaction Identifier shall be globally unique;
- Transaction Identifier shall be usable as a key identifier in protocols used in the Ua interface;
- NAF shall be able to detect the home network and the BSF of the UE from the Transaction Identifier.

NOTE: Care has to be taken that the parallel use of GBA and non-GBA authentication between UE and NAF does not lead to conflicts, e.g. in the name space. This potential conflict cannot be resolved in a generic way as it is dependent on specific protocol and authentication mechanism used between UE and application server. It is therefore out of scope of this specification.
For the example of HTTP Digest authentication used between UE and NAF, parallel use is possible as the following applies: <username,password>-pairs must be unique to one realm only. As the NAF controls the realm names, it has to ensure that only the GBA based realm is named with the reserved 3GPP realm name. In the special case that the NAF wants to allow non GBA based authentication in the GBA realm also, it has to ensure that no usernames in the format of a Transaction Identifier are used outside GBA based authentication.

~~Editor's note: Parallel use of GBA and non-GBA infrastructure is ffs. There are use cases when NAF may want to use GBA and non-GBA based infrastructures at the same time. For example, a NAF may want to authenticate subscribers both by using normal HTTP Digest authentication (where the usernames and passwords are distributed using some other mechanism than GBA), and by using GBA based HTTP Digest. However, it seems that in most telecommunication protocols, the server side (i.e. NAF) controls the name space related to key identifiers (cf. Transaction Identifier). For example, in HTTP authentication, the server issues the usernames, and does not allow the re-use of already existing usernames. The parallel use of GBA and non-GBA based infrastructures may cause conflicts on Transaction Identifier namespace. In particular, BSF may assign Transaction Identifier values that NAFs are already using with non-GBA UEs.~~

~~Editor's note: GBA shall further specify on how security associations are removed and/or updated in NAF.~~

*************** end change *********************************