Source: **SA1**

Title: **CR to 22.240 on Generic User Profile (Rel-6)**

Document for: **Approval**

Agenda Item: **7.1.3**

Meeting	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers. Current	Vers New	SA1 Doc
SP-21	SP-030469	22.240	001		Rel-6	F	Clarifications for section 7 of 22.240	6.0.0	6.1.0	S1-030965

CR-Form-v7

CHANGE REQUEST

⌘   **22.240** CR **001**   ⌘**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⌘ **X**   ME **X** Radio Access Network ☐   Core Network **X**

Title: ⌘	Clarifications for section 7 of 22.240		
Source: ⌘	Siemens		
Work item code: ⌘	GUP	***Date:*** ⌘	26/06/2003
Category: ⌘	**F**	***Release:*** ⌘	Rel-6

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.

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)*
   Rel-6 *(Release 6)*

Reason for change: ⌘	Requirements in section 7 of TS 22.240 need to be tidied up.
Summary of change: ⌘	Requirements in section 7 of TS 22.240 are tidied up. The wording is aligned to the rest of the document ("supplier" and "consumer" instead of "sender" and "recipient"). Requirement 6 has been reformulated for clarity
Consequences if not approved: ⌘	Unclear requirements could lead to misinterpretation by SA2, SA5 and T2

Clauses affected: ⌘	7			

		Y	**N**		
Other specs affected: ⌘		**X**		Other core specifications ⌘	23.240, 23.241
				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/specs/CR.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://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 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.

7 Security

Secure mechanisms shall be available for the transfer of User Profile data to, from or between authorised entities. Access to User Profile data shall only be permitted in an authorised and secure manner. The secure mechanisms to be applied shall be appropriate to the level of confidentiality of the data, the endpoints of the transfer and the routes that are available for the transfer of the data. The owner of the data, normally the body storing the master copy of the data, shall be responsible for applying the appropriate level of security to the transfer of the data.

The secure mechanisms available shall include the following:

1. Authentication of ~~recipient~~consumer
   Before any user data transfer takes place, it shall be possible for the ~~sender~~ supplier of the data to verify the identity of the ~~recipient~~consumer.

2. Authentication of supplier~~sender~~
   It shall be possible for the consumer ~~recipient~~ of data to identify the supplier~~sender~~.

3. It is permissible for either the supplier ~~sender~~ or consumer ~~recipient~~ of data to employ the services of a third party, known to, and trusted by, both in order to provide authentication of identity.

4. The validity of an authentication of identity shall, if required, be subject to a maximum time limit.

5. It shall be possible for the supplier ~~sender~~ of data to render the data to be unreadable by any party not authorised to receive it.

6. It shall be possible for the consumer ~~recipient~~ of data to detect whether the data have been tampered with during transmission. ~~the sender has made any change to the data subsequent to its transmission~~.

7. The security mechanisms shall provide verification that the data has been sent by the supplier ~~sender~~ and received by the consumer ~~recipient~~ (non-repudiation).

8. It shall be possible for the supplier ~~sender~~ and/or the consumer ~~recipient~~ to create an audit log of all GUP data transfer transactions of a specified type, provided that this requirement is made known before any transfer takes place

9. User profile data in general is proprietary data. This data may not be shared with unauthorized entities. *Access control* to the data is required. This access control must also apply to data which is located at legacy systems, currently without own access control functionality.

10. Correct setting of data values in the user profile may be critical for the integrity of certain network services. Therefore, *consistency checks* are needed to minimise the risk.

11. Transaction security for the change of data should be available in order to ensure the consistent change of data at different locations.